FUNDAMENTOS DE MATEMÁTICAS

colección notas de clase

notas notas notas notas notas notas

Fernando Zalamea

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE BOGOTÁ
FACULTAD DE CIENCIAS

Facultad de Ciencias
Saber más y formar mejor

Fundamentos de Matemáticas

Fernando Zalamea

Departamento de Matemáticas
Facultad de Ciencias

Universidad Nacional de Colombia
Sede Bogotá

FUNDAMENTOS DE MATEMÁTICAS

© Fernando Zalamea

Departamento de Matemáticas
Facultad de Ciencias
Universidad Nacional de Colombia

© Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas

Primera edición, 2007
Segunda reimpresión, 2012
Bogotá, Colombia

ISBN 978-958-701-831-8

Impresión: Proceditor
proceditor@yahoo.es
Bogotá, Colombia

Diagramación en LaTeX : Fernando Zalamea, con el soporte de Gustavo Rubiano
Gráficas interiores: Margoth Hernández y el autor
Diseño de carátula: Andrea Kratzer

x, 164 p. : 78 il.
ISBN 978-958-701-831-8

Índice general

Prólogo v

1. El mundo de las matemáticas: sorpresa, invención, rigor 1

1.1. La sorpresa 2

1.2. La invención 4

1.3. El rigor 7

1.4. Ejercicios 12

2. Conjuntos finitos y proposiciones 14

2.1. Conjuntos, pertenencia e inclusión 15

2.2. Proposiciones 19

2.3. Ejercicios 24

3. Conjuntos infinitos y cuantificadores 27

3.1. Conjuntos de números 27

3.2. Cuantificadores 31

3.3. Ejercicios 33

4. Relaciones y funciones 36

4.1. Relaciones 37

4.2. Funciones 42

4.3. Teorema de Cantor 47

4.4. Ejercicios 50

5. Operaciones entre conjuntos **54**

5.1. Complemento, unión, intersección, partes 55

5.2. Imágenes directa e inversa 57

5.3. Ejercicios 60

6. Tamaños de infinitud **62**

6.1. Inyecciones entre conjuntos infinitos 62

6.2. Ejercicios 67

7. Números naturales **68**

7.1. Axiomas y principio de inducción 68

7.2. Pruebas por inducción 70

7.3. Buen orden 74

7.4. Ejercicios 76

8. Números enteros y racionales **78**

8.1. Construcción de los números enteros 79

8.2. Más sobre divisibilidad en $\mathbb{Z}$ 86

8.3. Números racionales 89

8.4. Ejercicios 92

9. Números reales **94**

9.1. Sucesiones de racionales 94

9.2. Vecindades fundamentales 96

9.3. Completamiento de los racionales 98

9.4. Propiedades fundamentales de los reales 99

10.1. Los conjuntos de números 105
10.2. El universo conjuntista 107
10.3. Ejercicios 109

11.Más sobre reales **112**
11.1. Gráficas de funciones 113
11.2. Algebraicidad y trascendencia 122
11.3. Ejercicios 125

12.Polinomios y fracciones racionales **128**
12.1. Polinomios 128
12.2. Irreducibilidad 136
12.3. Fracciones racionales 138
12.4. Ejercicios 140

13.Números complejos **142**
13.1. Números complejos 143
13.2. Representaciones geométricas 144
13.3. Exponencial compleja 147
13.4. Ejercicios 151

14.Más sobre complejos **152**
14.1. Propiedades del conjunto de los complejos 152
14.2. Ejemplos de funciones de variable compleja 154
14.3. El teorema fundamental del álgebra 157
14.4. Ejercicios 160

Bibliografía anotada **163**

3); pero, a su vez, observamos que no contamos con las herramientas necesarias para el manejo del infinito, y nos abrimos a la relacionalidad y a la funcionalidad (capítulo 4); en otras instancias sucesivas, ya con esas herramientas en mano, aprendemos a *educar* nuestra frágil intuición infinitaria (capítulos 6 y 10). En forma similar, observamos cómo, «más allá» de las proposiciones (capítulo 2), requerimos cuantificadores (capítulo 3) para los manejos conjuntistas. Las diversas limitantes de los conjuntos de números dan lugar a las construcciones arquitectónicas de los enteros (capítulo 8), los racionales (capítulo 8), los reales (capítulo 9) y los complejos (capítulo 13), con las cuales se pueden ir *subsanando progresivamente* las diversas obstrucciones encontradas en cada piso del edificio numérico. Finalmente, se revisan algunas de las múltiples fronteras algebraicas que pueden explorarse gracias a manejos polinomiales (capítulo 12), hasta llegar a la «mejor resolución posible» de esas limitantes, con el teorema fundamental del álgebra para los números complejos (capítulo 14). A lo largo del texto, en el momento de introducir conceptos, pruebas o ejemplos, se enfatizará a menudo ese primer *motivo* fundamental, alrededor de las *limitantes del saber*, donde el proceder matemático tiene muchísimo para ofrecernos.

El segundo principio básico alrededor del cual evoluciona el texto consiste en manejar pragmáticamente las ***fronteras de la noción de demostración***. La *pragmática* consiste aquí en *ir y venir* alrededor de los supuestos bagajes previos del estudiante, sin nunca asumir del todo ni una determinada carencia, ni un determinado logro, sino *aumentando* a lo largo del texto su capacidad para manejar conceptos y para escribir pruebas ligadas a esos conceptos. La *evolución* de las pruebas es patente, empezando desde argumentos sencillos y bloqueos esperados (capítulo 1), pasando por pruebas más sofisticadas (teoremas de Cantor, capítulo 4; buen orden, capítulo 7; identidad de Bézout, capítulo 8), y llegando a la magnífica prueba de Gauss del teorema fundamental del álgebra (capítulo 14). En todo este proceso, *nunca* se alcanza un rigor formal (o «fundamentalista») de prueba, un rigor al que se irá acercando poco a poco el estudiante en su Carrera. Una supuesta «fundamentación definitiva» del saber matemático no es más que una *quimera*, y el estudiante deberá ir incesantemente revisando y reacondicionando la adquisición de sus conocimientos a lo largo de la Carrera. Sin embargo, luego de este primer acercamiento a la noción de demostración, se confía en que el estudiante será capaz de detectar *niveles de dificultad* en las pruebas, y de manejar cada nivel de acuerdo con los *problemas, conceptos, ejemplos y métodos* que se le provean.

Organización del curso. El material está diseñado para ser dictado en un semestre, en 14 semanas correspondientes a cada uno de los 14 capítulos, más un par de semanas adicionales para revisiones, o para ampliar con mayor comodidad el tiempo dedicado a alguno de los capítulos, a juicio del instructor. La organización de cada semana puede estructurarse alrededor de: (i) cuatro horas presenciales de clase magistral, donde el instructor presenta el material teórico, con abundantes ejemplos; (ii) dos horas presenciales de ejercicios con el instructor, ya sea en grupos o en forma individualizada; (iii) dos horas opcionales de ejercicios con el monitor. El estudiante promedio debe tener sin embargo *muy claro* que sin un número importante de horas *diarias* adicionales de estudio, por fuera del horario presencial de clase, no tendrá ningún éxito en un curso como FUNDAMENTOS. El estudiar eficiente y concienzudamente por fuera de clase resulta ser algo imprescindible, que el estudiante tendrá que saber sortear en los estudios universitarios *desde el primer semestre*.

El texto incluye un número muy amplio de ejercicios para trabajar en forma autocontenida, pero es también recomendable contar al tiempo con otros libros de precálculo o de teoría elemental de conjuntos (ver bibliografía anotada). Los ejercicios son parte *imprescindible* del texto, y constituyen el complemento natural, la extensión necesaria, de los desarrollos avanzados en el cuerpo expositivo principal. Debe señalarse aquí que los ejercicios del texto deben acompañarse de una importante cantidad adicional de cálculos particulares con objetos concretos. Ejemplos de esas situaciones aparecen en las tablas incluidas en el trabajo, pero deben completarse con diversos ejercicios adicionales de cálculo concreto. Cada instructor del curso debe ser *responsable* de esos ejemplos calculatorios e instrumentales, fundamentales para el estudiante. Éste, por su parte, siguiendo los ejemplos concretos del texto, y aquellos adicionales presentados en el tablero, puede (y debe) repetir situaciones similares con ligeras variaciones.

El uso repetido de expresiones *en cursiva* y de expresiones «entre corchetes» responde a los siguientes criterios precisos que debe tener en cuenta el estudiante: las cursivas enfatizan la importancia de una idea o un concepto, mientras que, en cambio, los corchetes se usan alrededor de ideas y conceptos que en el momento de su aparición aún no han sido definidos, y que, en la gran mayoría de los casos, no resultarán siquiera definibles en el curso completo de FUNDAMENTOS. Las palabras y los términos entre corchetes deben quedar sin embargo *resonando* para cursos superiores (pues, al fin y al cabo, la matemática constituye un entramado de *contraposiciones armónicas* en el ámbito de la inteligencia).

Otra recomendación importante consiste en leer, paralelamente, algunos libros de historia de la matemática. Sólo al descubrir y *ver* la matemática *encarnada* en las figuras de sus grandes inventores y gestores, puede empezar a sentirse la rica viveza y la extraordinaria ingeniosidad del pensamiento matemático. A lo largo del texto, el estudiante encontrará algunas notas a pie de página con brevísimos resúmenes de vida y obra de matemáticos que han cambiado los rumbos de la disciplina. Las notas sólo aparecen como una *incitación* a imprescindibles lecturas complementarias en historia de las matemáticas, que debe realizar el estudiante.

Como el estudiante observará repetidamente a lo largo del texto, estaremos delineando un panorama *esencialmente incompleto*, que sólo se irá precisando mejor a medida que el estudiante recorra la Carrera de Matemáticas. En muchos momentos del texto, *proyectamos* situaciones que habrán de entenderse plenamente sólo en ciertos cursos posteriores. Hemos intentado dejar claramente *explícitos* esos lugares de apertura hacia el futuro, ayudando así, en lo posible, a construir una *guía* que le pueda servir al estudiante para orientarse dentro de un relieve complejo, que a menudo no le permite ver sino infranqueables montañas en derredor.

Los procesos de aprendizaje, como irá descubriendo el estudiante, necesitan de una *permanente revisión* de los conceptos, definiciones, demostraciones y ejemplos en juego. El entendimiento no surge de una vez por todas, en forma absoluta o emanada de alguna iluminación superior, sino a través de una tarea paciente de *reelaboración constante*, producida por la dura *tenacidad* de los seres humanos. El edificio del saber va asentándose poco a poco, a partir de ideas intuitivas que van refinándose progresivamente. El hecho de contar con ejemplos intuitivos de reales en los primeros capítulos, por ejemplo, *no riñe* con que esos ejemplos vuelvan a ser reentendidos sobre *nuevas bases*, y con un rigor mayor, en los capítulos posteriores. El estudiante debe rehacer las demostraciones, primero observándolas, luego dejando de lado sus apuntes, y situándose sin más ayudas ante un papel en blanco. De la misma manera, los ejemplos y ejercicios que proveen los instructores en el tablero deben incesantemente reescribirse. *Escribir correctamente* (no sólo matemáticamente, sino *en español*) es un bagaje imprescindible en una *carrera de precisión* como la que emprende el estudiante (tanto una carrera contra el tiempo, como una Carrera disciplinar exigente). Un sabio manejo de las jornadas diarias de estudio y una dedicación plena a las labores universitarias son aquí primordiales. Muchos sacrificios son finalmente recompensados por la amplitud de miras, el rigor de pensamiento y la fluidez metodológica que consigue el matemático.

Agradecimientos. Estas notas de clase hubiesen sido imposibles sin la extraordinaria generosidad del Profesor Gustavo Rubiano. Gustavo puso a mi disposición todo su extenso conocimiento y su incesante ejercicio práctico del LaTeX, sin los cuales elaborar estas notas me habría tomado muchos semestres más. Sin el menor reparo, Gustavo me instaló los paquetes necesarios, me ayudó en los primeros pasos (mi conocimiento del LaTeX era, si se puede decir, antediluviano, habiendo realizado mi tesis doctoral en las primeras versiones del TeX, plagadas de comandos y sin interfaces gráficas), y, sobre todo, me ofreció los archivos completos correspondientes a sus libros, así como los macros que ha estado utilizando para sus propias publicaciones: una *inaudita amplitud* que nunca sabré agradecerle lo suficiente.

En segundo término, agradezco las extensas lecturas de este material por las Profesoras Myriam Acevedo, Margarita Ospina y Clara Helena Sánchez. Su conocimiento del curso, su amplia experiencia y sus enfoques pedagógicos orientaron muchas correcciones, numerosos esclarecimientos y algunas adiciones en el material. Las atentas lecturas de los Profesores Alexander Cruz, Arnold Oostra y Andrés Villaveces mejoraron también los ejemplos y la precisión del texto. Su extensa visión me permitió explicitar mejor los desarrollos y los eventuales aportes del trabajo. Es claro, sin embargo, que el encadenamiento de este material, así como todos los errores no vislumbrados y los énfasis adoptados quedan bajo mi única responsabilidad. Como consecuencia de las diversas miradas de mis colegas, se puede concluir que tal vez necesitemos renovar nuestro *curriculum* en las Carreras de Matemáticas a nivel colombiano (o latinoamericano). Ojalá este texto pueda situarse en esa dirección.

Agradezco aquí también a mis estudiantes del curso FUNDAMENTOS 2005-II, quienes supieron encarnar con humildad y trabajo el espíritu de este texto, así como a mis estudiantes del curso FUNDAMENTOS 2007-I, quienes ayudaron a enmendar una gran cantidad de erratas diversas, y pudieron responder a las exigencias filosóficas y conceptuales del texto, no fáciles para un primer semestre.

Finalmente, agradezco a Lorenzo Acosta, anterior Director del Departamento de Matemáticas, el que me incitara a acercarme al curso de FUNDAMENTOS, así como a Leonardo Rendón, actual Director del Departamento, por el reconocimiento de un tiempo precioso para elaborar estas NOTAS DE CLASE.

Capítulo 1

El mundo de las matemáticas: sorpresa, invención, rigor

Contenido

1.1. La sorpresa 2
1.2. La invención 4
1.3. El rigor 7
1.4. Ejercicios 12

En este primer capítulo presentamos algunas de las problemáticas profundas a las que debe abocarse el conocimiento matemático, y las ilustramos con algunos ejemplos clásicos derivados de la matemática griega. El manejo de ciertos razonamientos -en particular, la expansión imaginativa obtenida mediante las pruebas por contradicción- se entrelaza con conceptos, definiciones y ejemplos, alrededor de una idea fundamental que vertebra toda la disciplina: las matemáticas constituyen un instrumentario técnico y conceptual sofisticado para capturar *tránsitos y obstrucciones* entre el mundo físico real y las urdimbres ideales del saber.

1.1. La sorpresa

La matemática se mueve en una incesante oscilación pendular entre reconocer *singularidades y rupturas* dentro de un contexto dado y, luego, tratar de superarlas e integrarlas como *regularidades o continuidades* dentro de otro nuevo contexto ampliado. La fuerza del mundo real, con su enorme complejidad multiforme, donde todo es *mezcla*, subyace en los intentos de delimitación, análisis y conocimiento de esa realidad por diversas comunidades de intérpretes. Mediante múltiples filtros de representación, en el mundo alterno de las ideas se detectan entonces colecciones de estructuras y relaciones generales entre ellas, que dan lugar a valiosos *gérmenes* de orden, simetría y continuidad con los que se intenta comprender el *medio ambiente*, tanto natural como interpretativo, donde circulan los fenómenos y el saber.

Una de las hondas preguntas filosóficas detrás del conocimiento matemático consiste en cuestionarse acerca del irrazonable éxito de las construcciones *ideales* matemáticas en su aplicabilidad al mundo *real*. Aparentemente ajenas a la circunstancia, las matemáticas de los griegos, de los chinos, de los hindúes, de los árabes mantienen aún su vigencia y subsisten aún sus ejemplos, definiciones, teoremas. De forma muy diferente a lo que sucede en otros ámbitos de la cultura, donde no rigen ni la evolución ni la acumulación del saber, en las matemáticas se *avanza* en cambio en la elaboración de un gran edificio, donde a lo largo de la historia se acumulan fragmentos de conocimiento *universal* que trascienden sus acotados cronotopos de origen. Tanto los *acordes* como los *contrastes* entre lo ideal y lo real impulsan los desarrollos de las matemáticas, y una constante sensación de sorpresa nos sumerge al contemplar la *estabilidad* de nociones y conceptos matemáticos que habrían podido estar destinados al deterioro y al olvido.

Uno de los primeros grandes *desajustes* dentro del conocimiento matemático emerge cuando en la escuela de Pitágoras[1] se descubre que la diagonal d de un cuadrado de lado 1 es «inconmensurable» con el lado: no existen «números» a y b (para los griegos, números naturales mayores o iguales que 2) que «conmesuran» d y 1, es decir, tales que $d \cdot b = 1 \cdot a$. Mientras

---

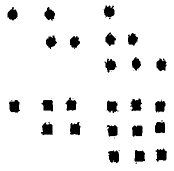
1 Pitágoras (Grecia, siglo VI a.C.) es uno de los fundadores de la matemática como método general del saber. Sabio universal, impulsó las conexiones de la matemática con la filosofía, la música y la cosmología.

que en las matemáticas previas a Pitágoras todo debía ser armonía y razón (como en el caso de las relaciones que el mismo Pitágoras encuentra entre las matemáticas y la música), el descubrimiento de la inconmensurabilidad de d introduce, con un ejemplo irrefutablemente sencillo, aquello que *no* es capturado por la razón. De hecho, si entendemos (con la matemática árabe medieval) los números racionales como primeras coordenadas de la razón, números que se expresan como razones a/b donde a y b son dos enteros ($b \neq 0$), el desajuste de la razón se expresa matemáticamente diciendo que $\sqrt{2}$ (igual a d por el teorema de Pitágoras) no es un número racional. En esas condiciones, emerge una gigantesca sensación de sorpresa en el pensamiento griego, a la vez que se abren los linderos fascinantes de la negación, del *revés* de la razón. Como veremos en la tercera sección de este capítulo, el hecho de que esos linderos de lo *no* dado se abran así al razonamiento y al riguroso control matemático constituye el comienzo de las altas aventuras del pensamiento matemático.

Ante un desajuste, una irregularidad, un desequilibrio, el matemático procede entonces a construir todo un gran andamiaje de conceptos, representaciones, definiciones, deducciones, ejemplos para captar parcialmente aspectos de la singularidad percibida. Esto da lugar a profundos desarrollos matemáticos donde la sorpresa inicial pasa a ser entendida con mayor propiedad, permitiendo explicar en parte los desajustes observados en una primera instancia. Una *ampliación en forma de espiral* es propia entonces del saber matemático: cada vez que se avanza a lo largo de la espiral del conocimiento, se regresa a la problemática inicial desde una nueva perspectiva, con nuevas herramientas que permiten ver más y mejor. En ese proceso, **no existe un fundamento último**, ni una visión superior única que resuelva todos los problemas.

Si la matemática se preocupa por un tipo de sorpresa ligada a lo singular, a lo incomprensible en primera instancia, una fuerte oscilación del péndulo la acerca de manera natural también al estudio de ciertas formas de *equilibrio* y de *simetría* con las que pueden codificarse regularidades profundas, tanto en el mundo real, como en el conjunto de urdimbres ideales con las que se intenta cartografiar esa realidad. La *geometría de los números* en la matemática griega combina de manera vistosa algunos ejemplos elementales de simetría.

Tanto los números cuadrados ($C_n = n^2$) como los números triangulares ($T_n = 1 + 2 + \ldots + n$), construidos gracias a claras representaciones geométricas, se combinan adecuadamente entre sí.



De hecho, una primera constatación recursiva permite observar que $T_n = T_{n-1}+n$, un tipo de enlace aritmético muy primario, que puede ser pronto superado por relaciones geométricas más interesantes. En efecto, un desplazamiento invertido de T_{n-1} sobre T_n muestra inmediatamente que $T_{n-1}+T_n = C_n$, así como otro desplazamiento muestra que $T_n+T_n = n(n+1)$, de donde $T_n = n(n+1)/2$.

La extensión infinita de ciertos conceptos es otra de las fuentes centrales de sorpresa en la matemática griega. La prueba clásica de la infinitud de los números primos (ver sección 3) -una joya de sencillez que se abre tanto al revés del razonamiento (prueba por contradicción) como al análisis estructural de un problema (factores y factorial)- abre compuertas insospechadas en la matemática. La prolongación indefinida, la extra-limitación de lo acotado incitan a la búsqueda prolongada e incesante de aquello que se nos escapa. La imaginación matemática empieza entonces a explorar oquedades, cesuras y fronteras del entendimiento de las que nunca podrá volver a retrotraerse.

1.2. La invención

Los cauces de la invención matemática son multiformes y multifacéticos. Un concepto matemático merece entenderse como un complejo hipercubo n-dimensional, que va siendo capturado progresivamente gracias a diversos cortes transversales. Las perspectivas desde las que se percibe cada corte cambian incesantemente, y es casi imposible entrelazar unitariamente todas las secciones a partir de las cuales podría reconstruirse el concepto completo.

La emergencia de la inventividad matemática estuvo, en los comienzos de la cultura griega, ligada profundamente con la filosofía. Herramientas, ambas, de comprensión general del mundo, buscaron en un mismo tiempo armonías y equilibrios entre el aparente caos circundante. Las *paradojas*

de Zenón de Elea[2] se inventaron como argumentos lógico-matemáticos sofisticados para sostener una posición filosófica fascinante pero difícilmente defendible: la visión parmenídea de que el *movimiento no existe* y de que la mayoría de nuestras percepciones no son más que *ilusiones* en un mundo estático, uno, permanente, sin flujos de ningún tipo. La lectura filosófica del mundo según Parménides va claramente en contra de nuestro *sentido común*, ya que sin cesar creemos percibir flujos, cambios, movimiento. Sin embargo, nuestro sentido común es el que podría estar engañándonos: nada, *a priori*, nos asegura que nuestra percepción no nos esté jugando una mala pasada. Los argumentos de Zenón intentan *abrir la posibilidad* de que las tesis de su maestro Parménides puedan representar una alternativa válida en la filosofía.

Zenón procede por un *argumento dialéctico*, que evoluciona hacia lo que pronto llamaremos *prueba por contradicción*. Zenón quiere demostrar que *no* hay movimiento; si sus contendores consideran que se trata de una posición absurda, él les demostrará que la posición de ellos tampoco puede considerarse como muy firme. Asuma, por lo tanto, que el movimiento sí existe. Suponga, por ejemplo, que hemos de lanzar una flecha entre un punto (A) y otro punto (B); la experiencia práctica y el sentido común nos aseguran que, con un buen arquero, la flecha se moverá, partirá de (A) y llegará a (B). Sin embargo, nos dice Zenón, para cubrir ese trecho, la flecha habrá antes de llegar a la mitad del camino, y, antes, a la mitad de la mitad de ese camino, y, antes, a la octava parte de ese camino, y, antes, a la dieciseisava parte del camino, *y así sucesivamente*. Siguiendo el razonamiento al infinito, la flecha no logrará superar entonces sus supuestos primeros desplazamientos y no podrá entonces empezar a moverse: el movimiento *no existe*, es una ilusión. Se trata de un argumento lógico-matemático sofisticado, una *invención que amplía los límites de la razón humana*, que no es fácil de rebatir de una manera rigurosa. Si confiamos en nuestro sentido común, sabemos que las paradojas de Zenón *tienen* que poder ser refutadas, pero no es fácil lograrlo mediante argumentos elementales. De hecho, sólo un pleno *control del infinito* permite resolver cuidadosamente las paradojas, algo que apenas

---

2 Zenón de Elea (Grecia, siglo V a.C.) es uno de los (muchos) ejemplos de cómo la filosofía ha ayudado en el crecimiento creativo de las matemáticas. La argumentación filosófica subyace escondida en la construcción de muchas conceptualizaciones (y, aún, de algunas maquinarias técnicas) propias de las matemáticas.

se conseguirá con la invención del cálculo diferencial e integral en el siglo XVII, más de 2000 años después de Zenón!

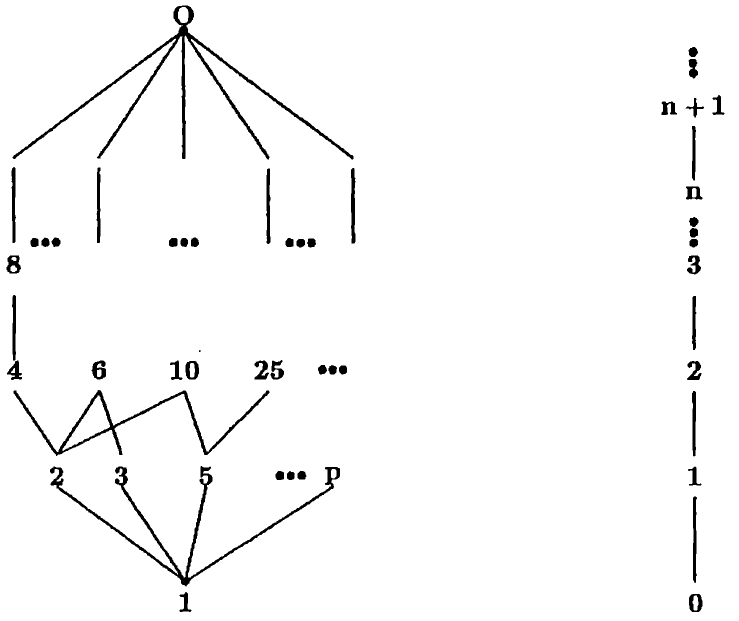
Las dos grandes corrientes impulsadas por el pensamiento matemático griego, ligadas a los desarrollos del número y del espacio, dan lugar a profundas invenciones en cada vertiente. Por el lado de los números, el solo tratamiento de las propiedades multiplicativas de los naturales da lugar a un complejísimo edificio. Consideremos, en efecto, al conjunto de los naturales, entendido intuitivamente, por ahora, con un comienzo en el 0 (ésta es una lectura posterior: los números, para los griegos, empezaban desde el 2) y generado por la operación de sucesor $n \mapsto n+1$. Denotemos por $|$ la relación de divisibilidad entre naturales ($n \mid m \Leftrightarrow$ existe k tal que $m = nk$). Esto da lugar, en términos modernos, al «retículo de divisibilidad de los naturales» (no importa no conocer por ahora la definición precisa de «retículo»: asúmase el término por el momento mediante la imagen de una red). Dentro de ese «retículo», se tienen relaciones muy interesantes. Empezando por lo más sencillo, por un lado $1 \mid n$ para todo n, pero por otro lado $n \mid 0$ para todo n. Si dibujamos la relación de divisibilidad en un plano, con flechas de abajo hacia arriba para indicar divisibilidad (por ejemplo $5 \mid 10$ da lugar a una flecha entre 5, situado abajo, y 10, situado arriba), esto significa que 1 está situado *por debajo de todos* los demás elementos, y que 0 está situado *por encima de todos*: son una suerte de mínimo y máximo elemento para la relación de divisibilidad (y, de hecho, son *exactamente* un mínimo y un máximo para la relación de *orden* de divisibilidad entre naturales, como veremos posteriormente).

La divisibilidad entre naturales da lugar a problemas muy complejos que se *aplanan* completamente si solo nos atenemos a la suma entre naturales. La *visión* de los «diagramas de Hasse»[3] asociados a cada una de esas relaciones (divisibilidad, por un lado, orden de la suma, por otro lado) señala fuertemente las diferencias en juego (ver diagramas). Rápidamente, se nos trastocan entonces nuestras supuestas certezas (¿0 es un comienzo o un final?: ambas cosas: inicio aditivo, final multiplicativo), y se amplían conside-

---

[3] Helmut Hasse (Alemania, 1898-1979) es uno de los brillantes matemáticos de la escuela alemana de la primera mitad del siglo XX, quienes, junto con David Hilbert, Emmy Noether y Emil Artin, fundaron el álgebra abstracta moderna. Sus contribuciones en teoría de números (y, en especial, en la «teoría de cuerpos de clases») fueron determinantes.

rablemente nuestros panoramas (¿qué tanto se abre hacia los lados y hacia arriba el «retículo» de divisibilidad?: mucho: ver ejercicios 1.8, 1.9). Entramos entonces en *ámbitos de la imaginación* de los cuales nunca querrá volver a escapar el matemático.



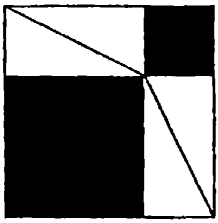
La invención matemática explota cuando se dirige particularmente hacia la *negación* del entorno finito y positivo del que emerge en primera instancia (matemática sumeria y egipcia). Con los griegos, lo no finito (el «apeiron»: lo infinito, lo ilimitado) y lo negativo (la dialéctica y el revés de los argumentos) amplían para siempre la capacidad inventiva de la razón humana. La superación de los pretendidos límites del mundo y de las limitantes del saber harán que la matemática no cese de explorar nuevos territorios de lo imaginario y de lo real. El *control* mismo ejercido con cada vez mayor precisión en esas exploraciones, mediante el rigor creciente de las demostraciones, permitirá seguir ampliando incesantemente un panorama inexhaustible.

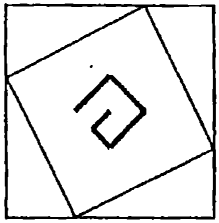
1.3. El rigor

Después de los procesos de la invención -o, mejor, *entrelazados* con ellos los procesos de prueba afianzan la práctica del matemático. Las pruebas no

surgen de una manera única, normativa o iluminadora, sino que emergen a través de andares y venires sinuosos, de rodeos por la oscuridad, de sedimentaciones y decantaciones. Las formas mismas de prueba cambian con el paso de los siglos. Hoy sabemos distinguir demostraciones completamente rigurosas de otras que lo son menos, gracias a una serie de avances en la formalización de la matemática, emprendidos desde mediados del siglo XIX hasta mediados del XX. Sin embargo, la demostración rigurosa ha limitado en algunos casos la capacidad de *visión*, libre y desprejuiciada, del matemático. Si observamos, a continuación, la demostración geométrica original del **teorema de Pitágoras** y una demostración algebraica más moderna del mismo, resulta inmediatamente evidente que la demostración antigua permite entender mejor (=*entrever*: ver a través de los intersticios) las simetrías y las regularidades en juego, mientras que, a su vez, la demostración moderna permite controlar mejor los pasos sutiles del razonamiento. Entre la *visión* y el *control* debe debatirse en buena medida la práctica matemática, y un adecuado *equilibrio* entre ambos resulta ser indispensable.

Prueba geométrica original. La redistribución de los cuatro triángulos (iguales) en las figuras siguientes muestra que el cuadrado construido sobre la hipotenusa es igual a la suma de los cuadrados construidos sobre los catetos:





Prueba trigonométrica/algebraica moderna. Dados a, b (catetos) y c (hipotenusa) como en cualquiera de los cuatro triángulos anteriores, sea α el ángulo entre el cateto medido por a y la hipotenusa (medida por c). Tenemos entonces: $\cos\alpha = a/c$, $\sin\alpha = b/c$, lo que implica $c\cos\alpha = a$, $c\sin\alpha = b$, por tanto $c^2\cos^2\alpha = a^2$, $c^2\sin^2\alpha = b^2$, es decir $c^2(\cos^2\alpha + \sin^2\alpha) = a^2 + b^2$, lo que equivale al teorema *general* de Pitágoras $c^2 = a^2 + b^2$.

Obsérvese sin embargo que esta prueba, basada en la ley básica de la trigonometría, $\cos^2\alpha + \sin^2\alpha = 1$, podría verse como una demostración que incorpora un círculo vicioso ya que esa ley básica consiste precisamente en una forma *específica* del teorema de Pitágoras, aplicada a un triángulo

rectángulo de catetos iguales a 1. De hecho, lo anterior sugiere el hecho (cierto) de que el teorema de Pitágoras y la ley básica de la trigonometría son proposiciones *equivalentes*, es decir demostrables la una a partir de la otra. En la edificación de la matemática, deberá entonces asumirse en algún momento uno de los dos enunciados como más elemental que el otro, y entonces, al demostrar el enunciado de más bajo *nivel de complejidad*, podrá rápidamente deducirse el otro con un argumento similar al indicado arriba.

Así como los estratos de información matemática se sedimentan unos sobre otros, los tipos de razonamiento lógico también se encadenan entre sí. Los argumentos dialécticos de Zenón dan lugar a *métodos* rigurosos de razonamiento. Las *pruebas por contradicción*, fundamentales para el desarrollo de la matemática griega, como inmediatamente veremos, esquematizan de manera muy sencilla la dialéctica de Zenón: para demostrar algo, *basta* con asumir lo contrario y llegar a una contradicción. Es lo que hace Zenón, al querer mostrar que no hay movimiento: asume lo contrario (la flecha se mueve) y llega a una contradicción (la flecha está en reposo). El esquema de la prueba se escribe entonces: (no p implica contradicción) implica p. En el capítulo 2 introduciremos unos operadores más cómodos de negación e implicación para poder *controlar* mejor este tipo de frases, y podremos observar cómo la prueba por contradicción se encuentra estrechamente ligada con la *prueba por contrarrecíproca*: para probar p implica q basta con probar que no q implica no p (atención a la fundamental *inversión* de los términos).

Podemos ahora *demostrar* la gran sinrazón que tanto perturbó a la escuela pitagórica, a saber que **la hipotenusa de un triángulo rectángulo de catetos iguales a 1 no puede ser medida por un número racional.** A partir del *teorema de Pitágoras* sabemos que $\sqrt{2}$ mide esa hipotenusa, pues $(\sqrt{2})^2 = 2 = 1^2 + 1^2$. Por otro lado, mediante una *prueba por contradicción*, procedemos a demostrar la irracionalidad de $\sqrt{2}$. Supóngase por tanto lo contrario, es decir que $\sqrt{2}$ es racional: $\sqrt{2} = \frac{a}{b}$, con a, b naturales, $b \neq 0$. Puede suponerse que a y b no tienen factores comunes (llamemos (*) a esta condición), ya que, si los tuvieran, esos factores comunes podrían eliminarse al simplificar repetidamente la fracción. A partir de $\sqrt{2} = \frac{a}{b}$ se deducen entonces las igualdades $b\sqrt{2} = a$ y, elevando al cuadrado, $2b^2 = a^2$ (**), por lo tanto a^2 es par. Ahora bien, si a^2 es par, entonces a es par: de hecho, una elemental *prueba por contrarrecíproca* muestra que si un número $2n+1$ es impar, su cuadrado $(2n+1)^2 = 4n^2+4n+1$ es impar. Tenemos entonces que $a = 2k$ y, reemplazando en la ecuación (**), se deduce $2b^2 = (2k)^2 = 4k^2$, por tanto $b^2 = 2k^2$, es decir que b^2 es par, lo que obliga a que b sea par. Se concluye que a y b son ambos pares, lo que *contradice* la condición (*).

La *riqueza* de la prueba anterior, más que en su manipulación ecuacional propiamente dicha, radica en el *entrelazamiento* de diversos *tipos* de prueba (contradicción, contrarrecíproca), de diversos *estratos* de prueba (argumento principal alrededor de la descomposición de $\sqrt{2}$, argumento secundario alrededor de la divisibilidad de un cuadrado por 2, hecho luego generalizable en forma idéntica para cualquier número primo), de diversos *ambientes* de conceptualización matemática (espacio y número, geometría y aritmética) y, finalmente, de diversos *contextos* de apertura para el conocimiento (mundos de posibilidad y fronteras de imposibilidad, limitaciones de las representaciones).

Otra antigua prueba griega, muy rica en información matemática y en sofisticación lógica es la demostración de la **existencia de una infinitud de números primos**. En términos modernos, la prueba se inscribe dentro del «retículo» de divisibilidad de los naturales (ver sección anterior). Un número primo, por definición, es un número mayor o igual que 2, cuyos divisores son solo 1 y el mismo número: p es primo si y sólo si $p \geq 2$ y $n \mid p$ implica $n = 1$ o $n = p$. La criba usual (Eratóstenes) para determinar el comienzo de la sucesión de los primos nos indica que 2, 3, 5, 7, 11, 13, 17, 19, 23, ... son números primos. Pero ¿cómo asegurar que la sucesión se extiende indefinidamente?

De nuevo, una *prueba por contradicción* es aquí muy útil. Supóngase, por contradicción, que sólo hay un número finito de primos. Sea p el mayor de esos números. Demostraremos que existe q primo, $q > p$, contradiciendo el hecho de que p era (supuestamente) el mayor de los primos. Obsérvese que los primeros ensayos ingenuos para construir ese número q, a partir de p, no funcionan: (1) si $q = p + 1$, q resulta ser par, por lo tanto no primo (pues p es impar, ya que todo primo estrictamente mayor que 2 debe ser impar: en efecto, por contradicción, si no lo fuese, sería divisible al menos por 1, 2 y $p(\neq 2)$, contradiciendo p primo); (2) si $q = p+2$, en algunos casos q podrá resultar primo (por ejemplo, en el caso de las parejas (p, q) iguales a (3,5), (5,7), (11,13), (17,19), etc.), pero en otros casos q no resultará ser primo (casos (7,9), (13,15), por ejemplo); de hecho uno de los grandes *problemas abiertos* en la aritmética consiste en saber si existe una infinitud de parejas $(p, p + 2)$ formadas por números primos (una famosa conjetura enuncia que sí existe una tal infinitud). Así, los primeros ensayos ingenuos que llevan a intentar construir q a partir de p, *sumando* algo, no llevan a ningún lado. Realmente, esto no es extraño, pues la *estructura* importante que está en juego es la estructura *multiplicativa* de los naturales (ligada a la relación de divisibilidad) y no la estructura aditiva. Puede entenderse que

surja entonces ahora en el curso de la prueba la idea de trabajar con $p!$, el número que, por definición, captura *toda* la estructura previa multiplicativa por debajo de p: $p! = 1 \cdot 2 \cdot 3 \cdot \cdots (p-2) \cdot (p-1) \cdot p$.

Claramente, $p!$ está lo más lejos posible de ser primo, pues tiene una enorme cantidad de divisores, pero considérese entonces, de nuevo ingenuamente, el número $p! + 1$. La prueba continúa, dividiéndose en *dos casos*. Primer caso: $p! + 1$ es primo; tómese entonces $q = p! + 1$, pues claramente $q = p! + 1 > p$. Segundo caso: $p! + 1$ no es primo (en principio, no tenemos modo de saber cuál de los dos casos va a darse, pero asumimos aquí una ley lógica fundamental: el *principio del tercio excluso*, según el cual algo *es o no es*). Si estamos en ese segundo caso y $p! + 1$ no es primo, debe entonces existir *otro* primo q que divide a $p! + 1$ (esto no es obvio en primera instancia, pero un argumento *iterado* de división debe llevar a convencernos de esa existencia). Afirmamos que para ese primo q se tiene entonces $q > p$, como se deseaba. Probamos de nuevo esto *por contradicción*. Supóngase que $q \leq p$; entonces q es un número entre 2 y p, por lo tanto divide a $p!$; pero q también dividía a $p! + 1$ (pues así fue cómo se construyó); entonces q divide a la resta de los dos números $((p! + 1) - p! = 1)$, es decir $q \mid 1$, contradicción con $q \geq 2$ (pues q es primo).

De nuevo, estamos ante una prueba de una enorme riqueza, tanto por la información matemática incluida, como por la *organización lógica* de la misma. El razonamiento en diversos estratos, las invocaciones sucesivas de pruebas y subpruebas por contradicción dan la medida de lo que puede empezar a vislumbrarse como la riqueza del pensamiento matemático. Ciertamente, comienza aquí a edificarse un muy complejo edificio. En lo que sigue de estas NOTAS DE CLASE se presentarán, aún de manera intuitiva, algunos de los FUNDAMENTOS elementales de ese edificio. A otros cursos posteriores (CONJUNTOS, LÓGICA) en la Carrera de Matemáticas les corresponderá estudiar los *Fundamentos* ya axiomáticos y rigurosos del edificio. Por ahora, en las NOTAS DE CLASE DE FUNDAMENTOS sólo nos adentraremos en algunos de los temas tocados en esta breve introducción:

(i) razonamientos lógicos proposicionales y conjuntos finitos

(ii) cuantificadores elementales y conjuntos infinitos

(iii) relaciones, funciones y operaciones entre conjuntos

(iv) construcciones de los conjuntos de números usuales.

1.4. Ejercicios

Nota. Los ejercicios de este primer capítulo enfrentan los diferentes bagajes de los estudiantes con la noción central de *demostración*. Se pretenden manejar aquí nociones *intuitivas* de prueba y de propiedades numéricas que, a lo largo del texto, se decantarán luego con todo el cuidado necesario. Las *obstrucciones naturales* que encuentren los estudiantes en estas primeras pruebas deberán irse subsanando paulatinamente a lo largo del curso. Aquí, dependiendo de cada nivel y de cada bagaje para cada estudiante del curso de FUNDAMENTOS, deberán producirse importantes *crisis*, que deberán ser poco a poco superadas. Sin una crisis (del griego *krisis*, «decisión»), y sin la *conciencia del no saber*, difícilmente puede procederse al saber, ya que sin una crisis es difícil *decidir conscientemente* qué caminos adoptar en el aprendizaje.

1.1. Demuestre que si p es primo, $\sqrt{p}$ es irracional (calque la prueba de que $\sqrt{2}$ es irracional, y use la *propiedad fundamental* de los números primos -ver ejercicio 1.5-: p primo y $p \mid ab$ implica $p \mid a$ o $p \mid b$).

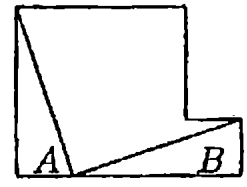
1.2. Demuestre que $\sqrt{6}$ es irracional.

1.3. Considere los números piramidales (o tetraédricos) P_n definidos por $P_n = T_1 + T_2 + \cdots + T_n$ (suma de los n primeros números triangulares). Explique visualmente el término asignado («piramidal») y *encuentre* (sin demostrarla) una fórmula general para P_n.

1.4. Demuestre la existencia de un par de números a, b tales que se tengan (a la vez): a, b irracionales, a^b racional. Ayuda: considere $\sqrt{2}^{\sqrt{2}}$ y realice un argumento por casos, dependiendo del resultado de esa exponenciación (racional o irracional).

1.5. Asumiendo el teorema de descomposición en primos (n natural, $n \geq 2$ implica que existen primos p_i y exponentes $\alpha_i \geq 1$ tales que $n = \prod p_i^{\alpha_i}$) demuestre que p es primo si y sólo si ($p \mid ab$ implica $p \mid a$ o $p \mid b$).

1.6. Estudie otra prueba visual del teorema de Pitágoras basada en los desplazamientos de los dos triángulos A y B en la figura adjunta:



1.7. Demuestre (para a, b, c naturales): $a \mid b$ y $a \mid c$ implica $a \mid b+c$, $a \mid b-c$, $a \mid bc$.

1.8. Proporcione ejemplos de números naturales situados en los niveles 8 y 9 del diagrama de Hasse de los naturales con divisibilidad. ¿Puede siempre situar *algún* natural en el nivel n del diagrama? ¿Puede situar *infinitos* naturales en cada nivel n?

1.9. ¿Existe algún natural $a \neq 0$ tal que en el diagrama de Hasse de los naturales con divisibilidad no exista ningún natural entre a y 0?

1.10. Recuerde que 0 es divisible por todo natural. Demuestre sin embargo, por contradicción, que 0 no divide a ningún natural diferente de 0.

1.11. Demuestre, por contradicción, que $3 \mid n^3$ implica $3 \nmid (n+1)^3$ (donde $\nmid$ significa no divide).

1.12. Demuestre, por contradicción, que no existen naturales $x, y \geq 1$ tales que $x^2 - y^2 = 1$.

1.13. Demuestre, por contradicción, que si los lados (no nulos) a, b, c de un triángulo satisfacen $a^2 + b^2 = c^2$ entonces el triángulo es recto (*contrarrecíproca* del teorema de Pitágoras).

1.14. Escriba con cuidado alguna de las paradojas de Zenón no señaladas en el texto, y explique cómo intenta Zenón demostrar *por contradicción* la imposibilidad del movimiento.

Capítulo 2

Conjuntos finitos y proposiciones

Contenido

2.1. Conjuntos, pertenencia e inclusión 15
2.2. Proposiciones 19
2.3. Ejercicios 24

Hemos visto en el capítulo precedente cómo la matemática se enriquece al empezar a explorar los linderos de la negación: lo no finito, lo no racional, lo no demostrable de manera positiva o elemental. Sin embargo, antes de adentrarnos en lo infinito y en lo no positivo/elemental, es importante *fijar* algunos núcleos de razonamiento primordial dentro de lo finito y lo elemental. En este capítulo presentamos la noción de conjunto desde un punto de vista intuitivo, concentrándonos por el momento en conjuntos finitos. Asociadas al manejo elemental de los conjuntos finitos, aparecen las combinaciones de proposiciones entre sí, es decir las manipulaciones intuitivas que subyacen al «cálculo proposicional clásico». El capítulo esencialmente precisa *un mínimo lenguaje de referencia* para poder expresar, representar y controlar lo finito y lo proposicional.

2.1. Conjuntos, pertenencia e inclusión

Desde un punto de vista intuitivo, las nociones de **conjunto** y de **elemento** *no pueden definirse* en una primera instancia. Su tratamiento axiomático está reservado para una comprensión posterior de los FUNDAMENTOS en la Carrera de Matemáticas. Para nosotros, se tratará entonces de dos *nociones primitivas*, que no pueden capturarse mediante un instrumentario de definiciones, pero que pueden ser caracterizadas por su *uso apropiado* (lo que, en otros contextos, se denomina su «pragmática»). Un «conjunto» y un «elemento» del conjunto deben verse intuitivamente entonces como un conglomerado (colección, amalgama, etc.) y como un ingrediente (punto, átomo, etc.) de ese conglomerado: una intuición ciertamente no muy diciente, que sólo la *práctica* logra resolver de manera eficaz. Un elemento de un conjunto se dice que *pertenece* al conjunto.

En una aproximación inicial, un conjunto puede ser definido de dos formas complementarias: por **extensión**, gracias a una *lista* completa de sus elementos, o por **intensión**, gracias a una *propiedad* que defina adecuadamente las características de los elementos del conjunto. Así, por ejemplo $A = \{1, 2\}$ por extensión, o $A = \{n \text{ natural} : 1 \leq n < 3\}$, o $A = \{n \text{ natural} \geq 1 : \text{existen } x, y, z \text{ naturales no nulos tales que } x^n + y^n = z^n\}$ definen al *mismo* conjunto A, por extensión o por intensión (la última representación está *muy lejos* de ser obvia, y requiere la prueba del famoso Teorema de Fermat[1]).

Esencialmente, los conjuntos matemáticos se definen mediante propiedades, a su vez expresables por fórmulas, es decir por intensión (o por «comprensión», como también se le llama a este proceso); los desarrollos matemáticos tienden luego a tratar de precisar la extensión correspondiente a las propiedades iniciales. En buena medida, el paso de lo implícito (intensional) a lo explícito (extensional) se convierte en una de las tareas centrales del pensamiento matemático. Por supuesto, un vaivén plenamente *pendular* entre lo intensivo y lo extensivo cubre perspectivas más amplias dentro de

---

1 Pierre de Fermat (Francia, 1601-1665) fue uno de los precursores del cálculo diferencial e integral, fundador de la teoría de las probabilidades y gran aficionado a la teoría de números, en una época en la que la matemática todavía podía ser desarrollada por hombres universales (Fermat era abogado de profesión).

la historia de la matemática, pero el tránsito de lo implícito a lo explícito debe entenderse como una suerte de honda corriente principal que afecta las mareas en la superficie.

La relación básica indefinible entre elementos y conjuntos es la **relación de pertenencia**. Denotamos $a \in A$ para indicar que a es un elemento del conjunto A (o que a pertenece a A) si a está en la lista de los elementos de A (cuando A está dado por extensión) o si a verifica las fórmulas definitorias de A (cuando A está dado por intensión). De manera complementaria, denotamos $a \notin A$ para señalar que a no pertenece a A. Nuestras *convenciones de notación* manejarán usualmente las minúsculas para elementos y las mayúsculas para conjuntos, pero, como pronto veremos, se trata sólo de convenciones genéricas, pues en muchos casos particulares intuitivos de gran importancia los conjuntos son elementos de otros conjuntos (y en realidad resulta que, en una *fundamentación* axiomática posterior, en la cual no podemos aquí adentrarnos, *todos* los conjuntos son *obligatoriamente* elementos de otros conjuntos).

Una vez dadas las nociones *indefinibles* de conjunto, elemento y pertenencia, podemos ahora sí proceder a *construir* y elevar el edificio mediante *definiciones*.

Definición 2.1. Sean A y B dos conjuntos. Decimos que A está **incluido** en B (o que A es subconjunto de B, o que A está contenido en B), lo que denotamos por $A \subseteq B$, si y sólo si todo elemento que pertenece a A es un elemento que pertenece a B. La relación $A \subseteq B$ entre conjuntos se llama la relación de **inclusión** (o de contenencia).

De manera complementaria, denotamos $A \not\subseteq B$ para indicar que A no está incluido en B. Es fundamental observar aquí (por ahora de manera intuitiva, explicaremos esto mejor en el capítulo 3) que $A \not\subseteq B$ corresponde a negar la frase (*todo* elemento de A es elemento de B), es decir, a afirmar que *existe algún* elemento de A que no es elemento de B.

Es fundamental distinguir aquí de manera muy clara los *signos* fundamentales de la escritura conjuntista, y no mezclarlos arbitrariamente. Las distinciones entre los signos positivos $\{$, $\}$, $\in$, $\subseteq$, $=$ son imprescindibles. En particular, nunca deben confundirse la pertenencia ($\in$, relación entre *un* elemento y *un* conjunto) y la inclusión ($\subseteq$, relación entre dos conjuntos, que involucra a *todos* los elementos del primer conjunto). A su vez, deben distinguirse claramente los signos negativos $\notin$, $\not\subseteq$, $\neq$, y, en particular, hay que distinguir la relación de no pertenencia (que solo se refiere a un elemento y a

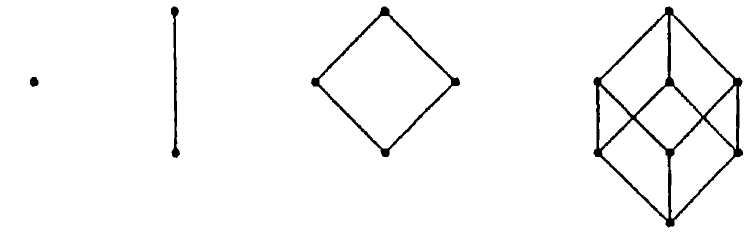
un conjunto *dados*) de la relación de no inclusión (que involucra una prueba de *existencia* de un elemento para separar a dos conjuntos). Merece señalarse aquí que el uso tradicional en matemáticas del término «símbolo» corresponde generalmente a una *degeneración* del término correcto («signo»): un *mal uso* que, en instancias superiores del pensamiento («semiótica»: teoría de los signos), lleva a considerables dificultades y que debe irse corrigiendo desde un comienzo.

Ejemplo 2.2. El conjunto **vacío**, denotado por $\emptyset$, se define como el conjunto *sin elementos*: su propiedad característica es que para todo a se tiene $a \notin \emptyset$, una propiedad que *incita* a trabajar con pruebas por contradicción. Para muchos objetos usuales A de la matemática se tiene que $\emptyset \notin A$ (aunque en el ejemplo siguiente veremos que $\emptyset$ sí pertenece a una ubicua colección de objetos en la matemática), pero, en cambio, *siempre* se tiene $\emptyset \subseteq A$ para todo conjunto A. Esto se puede confirmar observándolo por contradicción: $\emptyset \not\subseteq A$ equivaldría a asegurar que existiría *algún elemento en el vacío* que a su vez no fuese elemento de A, pero ya el comienzo de la frase es contradictorio pues no puede haber nada en el vacío.

Ejemplo 2.3. Sea A un conjunto. El conjunto **partes de** A, o conjunto potencia de A, denotado por $\wp(A)$, se define como el conjunto de los subconjuntos de A, es decir, de manera intensional: $\wp(A) = \{X : X \subseteq A\}$. Los *elementos* de $\wp(A)$ son aquí por tanto los *subconjuntos* de A: un mismo objeto es, en un nivel, subconjunto, y, en otro nivel superior, elemento. Para fijar las ideas, en el caso $A_2 = \{1, 2\}$, se obtiene, por extensión, $\wp(A_2) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ y en el caso $A_3 = \{1, 2, 3\}$, se obtiene $\wp(A_3) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$. El hecho de que $\wp(A_2)$ resulte ser un conjunto con cuatro elementos y de que $\wp(A_3)$ resulte tener ocho elementos indica un *patrón* de crecimiento *uniforme* del número de elementos de $\wp(A)$ a medida que aumenta el número de elementos de A. De hecho, puede intuirse que el número de elementos de $\wp(A_n)$ es exactamente 2^n si el número de elementos de A_n es n, algo que se confirma con los dos primeros casos: si $A_0 = \emptyset$, $\wp(A_0) = \{\emptyset\}$ tiene $1 = 2^0$ elemento, y si $A_1 = \{1\}$, $\wp(A_1) = \{\emptyset, \{1\}\}$ tiene $2 = 2^1$ elementos. La *prueba* de esta intuición, o de este patrón detectado, tomará más tiempo y requerirá de las herramientas fundamentales para poder hacer pruebas sobre el conjunto de los números naturales: las *pruebas por inducción* del capítulo 7.

Dentro de un conjunto de partes $\wp(A)$, dos elementos del conjunto de partes pueden compararse gracias a la relación de inclusión, ya que ellos mismos son conjuntos. Podemos entonces imaginar un diagrama de Hasse

en el cual un conjunto está por debajo de otro si el de abajo está incluido en el de arriba. De esta manera, es fácil obtener los primeros diagramas de Hasse para $\wp(A_n)$ con la relación de inclusión ($\subseteq$):



n = 0 n = 1 n = 2 n = 3

Obsérvese, en particular, el *cuadrado* obtenido para el caso $n = 2$ y el *cubo* obtenido para el caso $n = 3$: las representaciones *geométricas* obtenidas en los diagramas de Hasse de $\wp(A_n)$ se conectan plenamente con los cálculos *aritméticos* que miden el número de elementos. Se trata de una de las múltiples interconexiones entre espacio y número que recorren todo el tejido de la matemática.

Definición 2.4. Un conjunto A se dice **finito** si su lista extensional puede ser contada por un número natural. Veremos más adelante, en el capítulo 4, que esto quiere decir que A es del «mismo tipo» que alguno de los $A_n = \{1, 2, \cdots, n\}$, esto es, que puede ponerse en una adecuada correspondencia con A_n.

Una ventaja importante de un conjunto finito es que, a menudo, puede explicitarse el conocimiento del conjunto por extensión. Esto es algo que *nunca* podrá realizarse en cambio con los conjuntos infinitos, para los cuales ninguna lista puede en realidad concretarse (aún para conjuntos finitos de gran tamaño, la exhibición de una tal lista podría llegar a superar el número mismo de partículas en el universo, según algunos de los actuales modelos cosmológicos). En el infinito (o en finitudes de gran tamaño) no podemos entonces dejar de involucrarnos con *propiedades y relaciones* matemáticas, en vez de mantenernos en una cierta combinatoria de lo puntual como puede hacerse con algunos conjuntos finitos.

2.2. Proposiciones

Por medio del término **proposición**, entenderemos en este texto cualquier tipo de aserción *matemática* usual para la cual podemos intuitivamente afirmar que posee un valor verdadero (V) o falso (F). Por ejemplo, las aserciones 2 es un entero impar, $3 \mid 9$ (3 divide a 9), o $\emptyset \nsubseteq \emptyset$ son proposiciones, la primera con un valor falso, la segunda con un valor verdadero, la tercera con un valor falso. Las aserciones $2 \mid$, $x = 7$, o $A = \}1, 2$ no son proposiciones, ya que no son verdaderas ni falsas, la primera porque está incompleta (¿2 divide qué?), la segunda porque el valor de verdad dependerá de qué substituyamos por x, la tercera porque es una sucesión de signos gramaticalmente incorrecta. Denotaremos usualmente por p, q, r, ... ciertas proposiciones genéricas: estos signos se denominan **letras proposicionales.**

Restringiremos aquí la noción de «proposición» al *mundo matemático elemental*, y no nos andentraremos en el manejo más vago de proposiciones aplicadas a eventos externos del mundo en general, que adquieran valores verdaderos o falsos, como por ejemplo «ahora llueve», o «mi padre canta». Son tantos los ejemplos y es tan amplio el universo de las matemáticas que, en primera instancia, no sólo no es necesario salir de ese mundo, sino que es altamente recomendable *sumergirse plenamente* en él, en un primer curso de FUNDAMENTOS.

La trama de los razonamientos lógicos elementales, como vimos en el primer capítulo, está en buena medida determinada por ciertas transferencias de información ligadas a las ideas de negación y de implicación. A continuación, convertimos esas transferencias en *operadores* precisos sobre los que puede establecerse un adecuado control matemático.

Definición 2.5. Sean p, q letras proposicionales. Definimos los **conectivos** proposicionales negación ($\neg$), implicación ($\rightarrow$), conjunción ($\wedge$), disyunción ($\vee$) y equivalencia ($\leftrightarrow$) mediante las siguientes tablas definitorias (**tablas de verdad**):

p	$\neg p$
V	F
F	V

p	q	$p \to q$	$p \wedge q$	$p \vee q$	$p \leftrightarrow q$
V	V	V	V	V	V
V	F	▶F	F	V	F
F	V	V	F	V	F
F	F	V	F	F	V

Obsérvese que si queremos pensar en los conectivos como operadores que mantienen (en algunos casos) o intercambian (en otros casos) lo verdadero y lo falso, para cubrir todos los casos tendremos que estar construyendo tablas cuyo número de líneas es una potencia de 2, pues tendremos que recorrer el conjunto $\{V, F\}$ tantas veces como tengamos letras proposicionales. Este resulta ser el caso en las definiciones anteriores, con una tabla de dos líneas para el operador de negación (aplicado a una sola letra proposicional), y con una tabla de cuatro líneas para los demás operadores (aplicados a dos letras proposicionales). Obsérvese que, aunque aquí sólo nos ocupamos de los 4 conectivos binarios más usuales ($\to$, $\leftrightarrow$, $\wedge$, $\vee$), hay en realidad $2^4 = 16$ conectivos binarios posibles. No nos ocuparemos de todas estas posibilidades aquí (aunque véase el ejercicio 2.10).

El punto crucial en las definiciones anteriores de los conectivos se encuentra señalado con ▶ en la tercera línea de la segunda tabla. Todas las definiciones dadas en las tablas de verdad corresponden a nuestras intuiciones naturales, *excepto* en el caso de la implicación matemática. La implicación, *dentro del ámbito de las matemáticas elementales*, se entiende a través de un paradigma fundamental: lo único que se le pide en matemáticas a una implicación correcta es que *no transforme verdades en falsedades*. Todo el resto puede en cambio ser perfectamente razonable desde un punto de vista matemático. Esa apertura a todo lo otro, *al mundo de todos los posibles*, es imprescindible para la inventividad matemática. Obsérvese que esta mirada es bastante diferente del manejo más ambiguo que tienen las «proposiciones» lingüísticas, donde, por ejemplo, una frase del tipo «si mi padre es mi hijo entonces yo soy el padre de toda la humanidad» no tiene ningún sentido, mientras que si la *esquematizamos matemáticamente* como una implicación entre letras proposicionales, la primera falsa y la segunda falsa, la frase completa resulta ser verdadera. No enfrentaremos aquí este tipo de *extrapolaciones* al lenguaje coloquial diario, que nos acercan al absurdo, ya que nos restringiremos solamente a las «proposiciones» de la matemática.

Mediante combinaciones de conectivos y de letras proposicionales pueden construirse proposiciones más sofisticadas. Sin entrar en una rigurosa definición («recursiva») de tales combinaciones (algo que se realizará en los cur-

sos posteriores de LÓGICA), llamaremos **fórmulas** a aquellas combinaciones construidas a partir de letras, conectivos y paréntesis de forma «coherente e iterada». La práctica provee numerosos ejemplos y un control natural en la conformación de las fórmulas, sin necesidad de muchas elaboraciones: por ejemplo, las cadenas de signos $p \to (q \to p)$, $(p \to q) \to p$, $p \wedge \neg p$, $p \vee \neg p$, $p \to (p \vee q)$ son todas fórmulas. Hay que resaltar aquí que las fórmulas sólo se refieren a la adecuada construcción *gramatical* de la cadena lingüística y no a su posible sentido, ya sea éste verdadero o falso. Por otro lado, ciertas cadenas de signos como $p \to$, $\neg(\vee p)$, $q \vee \to p$ son ejemplos de cadenas gramaticalmente incorrectas, es decir, no son fórmulas.

Definición 2.6. Una fórmula es una **tautología** si, al realizar su tabla de verdad, todas las entradas en la columna final de la tabla (correspondiente a los valores de verdad de la fórmula) son entradas verdaderas.

Las tautologías representan por tanto formas de razonamiento *siempre verdaderas*, cuando las aplicamos al mundo clásico elemental de las matemáticas. Debe señalarse sin embargo aquí que, más allá de lo clásico y de lo elemental, existe un gran número de *lógicas no clásicas* que gobiernan *otros* espacios de las matemáticas. En esos ámbitos alternos -no abordados en el curso de FUNDAMENTOS, pero tampoco, desafortunadamente, en las carreras usuales de Matemáticas- muchas tautologías clásicas dejan de valer.

Ejemplo 2.7. Los razonamientos por *contradicción* y por *contrarrecíproca* corresponden a esquematizaciones proposicionales (fórmulas) que son *tautologías*. Podremos entonces usar las pruebas por contradicción y por contrarrecíproca de manera totalmente segura en el ámbito clásico de las matemáticas elementales. Esta *codificación* de hechos generales (razonamientos en el mundo de las matemáticas) por medio de hechos particulares (ciertas fórmulas que resultan ser tautologías), y la *consiguiente extrapolación* de esas certezas locales al universo global de la matemática, muestran la riqueza del proceder matemático.

En efecto, obsérvese que la prueba por contradicción corresponde al esquema $(\neg p \to (q \wedge \neg q)) \to p$, y que la prueba por contrarrecíproca corresponde al esquema $(\neg q \to \neg p) \to (p \to q)$. Realizando las tablas de verdad correspondientes a ambas fórmulas se concluye inmediatamente que ambas son tautologías.

p	q	$\neg q$	$q \wedge \neg q$	$\neg p$	$\neg p \to (q \wedge \neg q)$	$(\neg p \to (q \wedge \neg q)) \to p$
V	V	F	F	F	V	V
V	F	V	F	F	V	V
F	V	F	F	V	F	V
F	F	V	F	V	F	V

p	q	$\neg p$	$\neg q$	$\neg q \to \neg p$	$p \to q$	$(\neg q \to \neg p) \to (p \to q)$
V	V	F	F	V	V	V
V	F	F	V	F	F	V
F	V	V	F	V	V	V
F	F	V	V	V	V	V

Ejemplo 2.8. Otros ejemplos importantes de tautologías corresponden a las siguientes fórmulas:

$p \vee \neg p$ (ley del tercio excluso)

$\neg\neg p \to p$ (ley de la doble negación)

$(p \to q) \leftrightarrow (\neg p \vee q)$ (implicación a partir de negación y disyunción)

$(p \wedge q) \leftrightarrow \neg(\neg p \vee \neg q)$ (leyes de De Morgan).

En efecto, resulta muy fácil chequear que las tablas de verdad correspondientes a estas fórmulas son tablas de verdad de tautologías.

Ejemplo 2.9. Ya que, al azar, no es fácil que las tablas de verdad terminen en columnas con entradas verdaderas, *parecería* que la «mayoría» de las fórmulas no fueran tautologías (sin embargo, véase el ejercicio 2.11). Algunas fórmulas que *no* son tautologías, y que corresponden a *errores típicos de razonamiento* son las siguientes:

$(\neg p \to \neg q) \to (p \to q)$

$(\neg p \to q) \to (p \to \neg q)$

$(p \to (q \vee r)) \to (p \to q)$.

Podemos ahora *desglosar* la relación básica de contenencia entre conjuntos de la siguiente manera, haciendo entrar explícitamente en juego las nociones fundamentales de este capítulo (conjunto, elemento, contenencia, pertenencia, implicación) y una de las nociones fundamentales del próximo capítulo (cuantificador universal «para todo»):

conjunto	*contenencia*	*conjunto*
A	$\subseteq$	B

si y sólo si

(para todo a)	$a \in A$	$\rightarrow$	$a \in B$
cuantificador	*pertenencia*	*implicación*	*pertenencia*

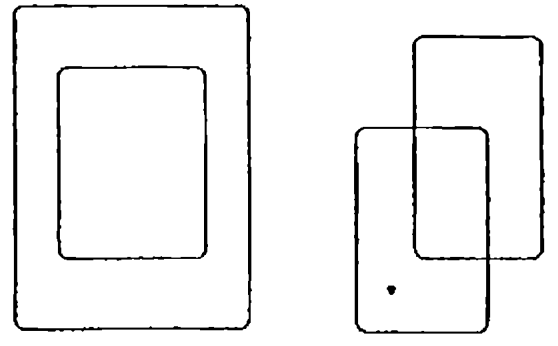
Hay que observar la *gran diferencia* que se tiene entre el análisis o desglose de la relación de *inclusión* (que involucra al cuantificador universal «para todo», la implicación y la pertenencia positiva), y el análisis de la relación de *no inclusión*, que involucra el cuantificador existencial «existe», la conjunción y la pertenencia negativa:

conjunto	*no contenencia*	*conjunto*
A	$\not\subseteq$	B

si y sólo si

(existe a)	$a \in A$	$\wedge$	$a \notin B$
cuantificador	*pertenencia*	*conjunción*	*no pertenencia*

La diferencia entre el *recto* ($\subseteq$)y el *verso* ($\not\subseteq$) de la situación puede *verse* mediante los útiles y bien conocidos diagramas de Venn:



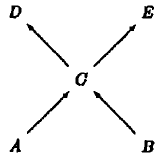
Obsérvese cómo en el primer diagrama (inclusión) se representa un patrón *general* (líneas unas dentro de otras), mientras que el segundo diagrama representa una situación *particular* (un punto situado en una franja específica). Pasaremos a estudiar en el próximo capítulo esas nociones de generalidad y particularidad, codificadas en los cuantificadores universal y existencial.

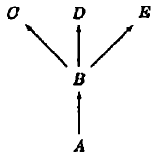
En los anteriores análisis y desgloses de los signos, éstos nunca deben confundirse, ni mezclarse *sin control*. La contenencia funciona entre conjuntos, no tiene sentido entre proposiciones. La implicación funciona entre proposiciones, no tiene sentido entre conjuntos. Un cuantificador habla sobre los elementos de un conjunto, no tiene sentido cuantificar proposiciones. Y así sucesivamente. La claridad en el manejo de los signos (y, por lo tanto, de los conceptos) es un *imperativo* en el curso de FUNDAMENTOS y en toda la Carrera de Matemáticas.

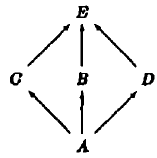
Por otro lado, tanto el estudiante, como cualquier instructor, deben entender claramente que, en un curso inicial como un curso de FUNDAMENTOS, es *sana*, diríamos casi indispensable, una cierta *mixtura* entre un lenguaje informal y fragmentos de nuevos lenguajes que intentan *progresivamente* introducir controles contextuales. El problema no se encuentra en las mezclas, sino en el *descontrol* que se tenga al manejar esas mezclas. Poco a poco el estudiante sabrá ir encontrando un adecuado *equilibrio* entre lo informal y lo formal, así como analizarlo rigurosamente. Toda la Carrera de Matemáticas le llevará a estudiar ese *deslinde*. A menudo, entonces, en lo que sigue del texto, combinaremos ciertas expresiones semiformales, con expresiones informales. De hecho, al revés de lo que a menudo se cree, la matemática es esencialmente *impura*, y en sus mezclas radica toda su energía. Todo esto conduce hacia un perfectamente manejable y pragmático **rigor informal** que es aquel que se quisiera poder implementar en un curso como FUNDAMENTOS.

2.3. Ejercicios

2.1. Proporcione ejemplos concretos de conjuntos A, B, C, D, E, que verifiquen las siguientes relaciones de inclusión (donde una flecha ascendente corresponde a una inclusión $\subseteq$, y donde la ausencia de líneas en un mismo nivel corresponde a no inclusión):







2.2. Encuentre todos los subconjuntos de $A_4 = \{1, 2, 3, 4\}$ y realice el diagrama de Hasse de $(\wp(A_4), \subseteq)$ (conjunto de partes con la relación de inclusión entre los subconjuntos).

2.3. Averigüe si las siguientes aserciones son verdaderas o falsas, justificando en cada caso sus respuestas:

(i) $\emptyset \in \wp(\wp(X))$ para todo conjunto X

(ii) $\{\emptyset\} \in \wp(\wp(X))$ para todo conjunto X

(iii) $\{\{\emptyset\}\} \in \wp(\wp(X))$ para todo conjunto X.

2.4. Exhiba algún conjunto X para el cual $X \nsubseteq \wp(X)$. Demuestre que, para cualquier conjunto finito X, $\wp(X) \nsubseteq X$.

2.5. Sea X un subconjunto de números naturales. Demuestre que si $X \subseteq \wp(X)$ entonces $X = \emptyset$ (ayuda: pruébelo por contrarrecíproca).

2.6. Dé ejemplos de conjuntos A, B, C tales que $A \in B \subseteq C \in A$. ¿Alguno de esos conjuntos puede verse como un conjunto conocido de números?

2.7. Demuestre que las fórmulas del ejemplo 2.8 son tautologías. Demuestre que las fórmulas del ejemplo 2.9 no son tautologías.

2.8. Decida si las siguientes fórmulas son, o no, tautologías, y demuéstrelo en cada caso:

$(p \vee q) \leftrightarrow (\neg p \rightarrow q)$

$((p \rightarrow q) \rightarrow p) \rightarrow p$

$(p \rightarrow (p \rightarrow p)) \rightarrow p$

$(p \rightarrow q) \vee (q \rightarrow p)$.

2.9. Demuestre que el conectivo $\neg$ no puede ser definido a partir de los conectivos $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, es decir, que no existe ninguna fórmula construida sólo con p y $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ que sea equivalente a $\neg p$. Ayuda: proceda por contradicción y observe el comportamiento de las combinaciones de $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ para el valor de verdad V.

2.10. Descubra cuáles son las dos únicas posibilidades de tablas de verdad para un conectivo *binario* $\boxplus$ que pretenda poder reconstruir, con sólo combinaciones del *mismo* conectivo $\boxplus$, a *todos* los demás conectivos (piense, en particular, en las exigencias que tienen que asumirse para poder reconstruir la negación: considere combinaciones de $\boxplus$ y p y compárelas con $\neg p$).

2.11. Explique por qué, *aparentemente*, hay más fórmulas no tautológicas que fórmulas tautológicas. Sin embargo, intente explicar por qué, *en realidad*, hay exactamente tantas tautologías como no tautologías.

2.12. Defina una familia $\alpha_1, \alpha_2, \ldots$ de fórmulas de la manera siguiente: $\alpha_1 = (p \to p)$, $\alpha_{n+1} = (\alpha_n \to p) \to p$. ¿Qué puede decir de los α_n: son o no tautologías, y por qué?

Capítulo 3

Conjuntos infinitos y cuantificadores

Contenido

3.1. Conjuntos de números 27
3.2. Cuantificadores 31
3.3. Ejercicios 33

Una vez concretado un cierto *núcleo* finito / proposicional de las matemáticas elementales, como lo hicimos en el capítulo anterior, podemos ahora sí tratar de empezar a expandirnos hacia sus bordes: hacia lo no finito y hacia lo no proposicional, es decir hacia lo *infinito* y lo *cuantificacional*. La idea fundamental es que, una vez entrados en el mundo de los conjuntos infinitos (como es el caso de los principales conjuntos de números, de los que nos ocupamos en el curso de FUNDAMENTOS), un primer control del infinito se consigue, de manera positiva, mediante el cuantificador universal, y, de manera negativa, mediante el cuantificador existencial. Un segundo control se obtendrá, en los capítulos posteriores, mediante las nociones de relación y función.

3.1. Conjuntos de números

Presentamos aquí de manera intuitiva los principales conjuntos de números, e introducimos los símbolos usuales para representarlos:

Naturales: $\mathbb{N} = \{0, 1, 2, 3, \cdots, n, n+1, \cdots\}$.

Se trata de los números desarrollados a partir del cero (0), mediante sumas sucesivas de una unidad (proceso sucesor: $n \mapsto n+1$).

Enteros: $\mathbb{Z} = \{\cdots, -n-1, -n, \cdots, 0, \cdots, n, n+1, \cdots\}$.

Se trata de los números naturales y de sus inversos para la suma (números negativos).

Racionales: $\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge b \neq 0\}$.

Se trata de los números enteros y de sus inversos para la multiplicación (fracciones), cuando esa inversión es posible.

Reales: $\mathbb{R}$ = «completamiento» de los racionales.

Se trata de los racionales y de números adicionales (expansiones decimales no periódicas) que intentan cubrir los «huecos» existentes en la línea racional («discreta»), para convertirla en un «continuo».

Por construcción, tenemos una cadena de conjuntos: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, con claras contenencias estrictas en cada caso:

$\mathbb{Z} \nsubseteq \mathbb{N}$ pues, por ejemplo, $-1 \in \mathbb{Z}$ y $-1 \notin \mathbb{N}$;

$\mathbb{Q} \nsubseteq \mathbb{Z}$ pues, por ejemplo, $\frac{1}{2} \in \mathbb{Q}$ y $\frac{1}{2} \notin \mathbb{Z}$;

$\mathbb{R} \nsubseteq \mathbb{Q}$ pues, por ejemplo, $\sqrt{2} \in \mathbb{R}$ y $\sqrt{2} \notin \mathbb{Q}$.

Obsérvese cómo las no contenencias se establecen mediante *ejemplos*, es decir mediante objetos existenciales concretos, tal como lo señalábamos al final del capítulo anterior.

Para cada uno de los conjuntos de números anteriores, pueden describirse múltiples subconjuntos *notables* de esos conjuntos dados. Dentro de los naturales, por ejemplo, son muy útiles los subconjuntos formados por primos, pares, impares, o múltiplos de un número dado: $\{n : n \in \mathbb{N} \wedge n \text{ es primo}\}$, $\{n : n \in \mathbb{N} \wedge n \text{ es par}\}$, $\{n : n \in \mathbb{N} \wedge n \text{ es impar}\}$, $m\mathbb{N} = \{n : n \in \mathbb{N} \wedge n \text{ es múltiplo de } m\}$. Obsérvese que cada uno de los subconjuntos anteriores es infinito, excepto en el caso de los múltiplos de 0, donde $0\mathbb{N} = \{0\}$. El único caso delicado es el de la infinitud de los primos, que demostramos ya en el capítulo 1. Dentro de los enteros, son de fundamental importancia, como veremos en diferentes instancias a lo largo del curso, los subconjuntos de múltiplos de un número dado: $m\mathbb{Z} = \{n : n \in \mathbb{Z} \wedge n \text{ es múltiplo de } m\}$. Distinga los subconjuntos de múltiplos en $\mathbb{N}$ y en $\mathbb{Z}$: por ejemplo, $3\mathbb{N} = \{0, 3, 6, \cdots, 3n, \cdots\}$, mientras que $3\mathbb{Z} = \{\cdots, -3n, \cdots, -3, 0, 3, \cdots, 3n, \cdots\}$.

Definición 3.1. Un conjunto es **infinito** si contiene un subconjunto «similar» a $\mathbb{N}$. Intuitivamente, el conjunto es infinito si un listado de sus elementos, sin repeticiones, no se acaba. En el capítulo 4 introduciremos las herramientas para definir rigurosamente la noción de «similaridad» y en el capítulo 6 revisaremos con cuidado las similaridades y las *no* similaridades entre los conjuntos infinitos usuales.

Ya que $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, los conjuntos de números enteros, racionales y reales son infinitos puesto que contienen un subconjunto similar a $\mathbb{N}$, a saber *el mismo* $\mathbb{N}$. Los conjuntos de múltiplos $m\mathbb{Z}$ (para $m \neq 0$) son también infinitos puesto que sus subconjuntos $\{0, m, 2m, 3m, \cdots\}$ son similares a $\{0, 1, 2, 3, \cdots\} = \mathbb{N}$. De hecho, como indicaremos en el capítulo 6, la propiedad de que un conjunto sea similar a una de sus *partes propias* (como el caso de $\mathbb{N}$ similar a $3\mathbb{N}$) es otra manera de *caracterizar* a los conjuntos infinitos (definición 6.3). Esta peculiaridad de los conjuntos infinitos se hace visible en la famosa «paradoja» de Galileo, según la cual, por un lado, hay *más* números naturales que pares (puesto que en la colección de los naturales aparece 3, mientras que en la de los pares 3 no aparece), pero, por otro lado, los naturales y los pares pueden contarse por *igual* ya que los podemos asociar uno a uno en los dos conteos «similares»

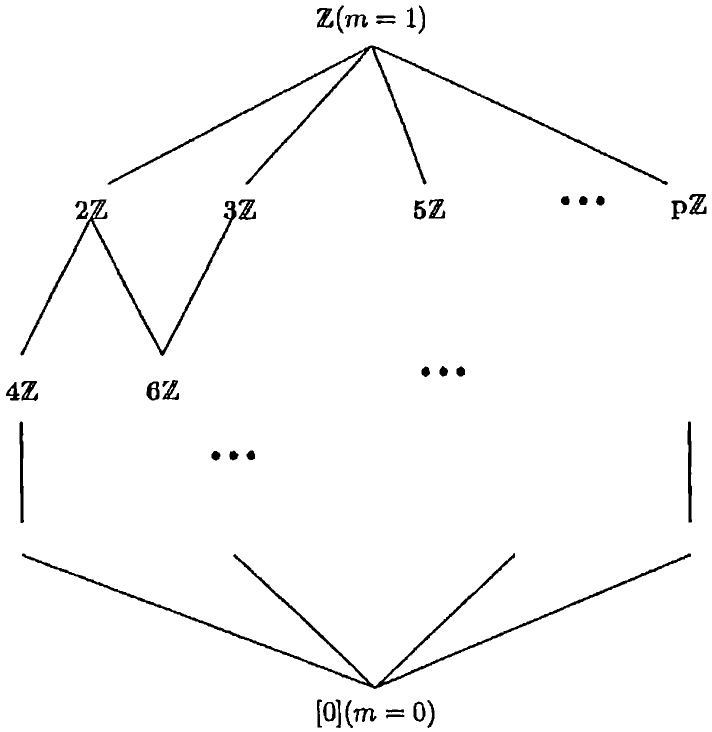
0	1	2	3	n	$n+1$
0	2	4	6	$2n$	$2n+2$

La propiedad paradójica de poder asociar la «parte» al «todo» es característica de los conjuntos infinitos, y, como veremos más adelante, consiste en el *corazón* mismo de lo infinito. La bellísima frase de Pascal[1], «el corazón posee razones que la razón no conoce», no sólo debe abrirnos a una *razón extendida a la imaginación*, como lo hemos señalado en el capítulo 1, sino que puede aplicarse a la comprensión compleja misma de la infinitud: el infinito posee razones que la razón finita no conoce.

---

[1] Blaise Pascal (Francia, 1623-1662) es uno de los exponentes mayores del gran espíritu de fineza del pensamiento francés. Notable filósofo, matemático y ensayista, su pluma y su razón son ejemplo de extrema concisión y claridad. El estudiante no podrá sino aprender exponencialmente, al acercarse, aunque sea vagamente, a la limpieza mental y expresiva de Pascal.

En el caso de un conjunto infinito X, la colección de sus subconjuntos (
decir, $\wp(X)$) no puede diagramarse de manera tan sencilla como lo hicim
en el capítulo 2 para los conjuntos $A_n = \{1, 2, \cdots, n\}$. Veremos en el próxin
capítulo que, en realidad, $\wp(X)$ literalmente *explota* cuando X es infinit
Sin embargo, ciertas colecciones de subconjuntos de un conjunto pueden
veces diagramarse bien, como es el caso de los subconjuntos de múltiplos m
($m \geq 0$) contenidos en $\mathbb{Z}$ (en el diagrama siguiente, las líneas ascendent
corresponden a inclusiones):



El estudiante podrá observar lo mucho que este diagrama se parece
tructuralmente al diagrama de Hasse de $(\mathbb{N}, |)$ (naturales con la relación
divisibilidad) que introdujimos en el capítulo 1. De hecho, los diagramas s
exactamente *inversos* uno del otro, y coinciden perfectamente si se los tr
lapa por medio de una reflexión. Esta *inversión* de los dos diagramas pue
expresarse de una manera completamente precisa mediante la constataci
fundamental:

$$m\mathbb{Z} \subseteq n\mathbb{Z} \quad \text{si y sólo si} \quad n \mid m.$$

En efecto, si $m\mathbb{Z} \subseteq n\mathbb{Z}$ entonces, como $m \in m\mathbb{Z}$, resulta $m \in n\mathbb{Z}$, es decir $m = nk$ para algún k, por tanto $n \mid m$. Viceversa, suponga que $n \mid m$; esto implica inmediatamente que todo número divisible por m es divisible por n, es decir que todo múltiplo de m es múltiplo de n: $m\mathbb{Z} \subseteq n\mathbb{Z}$.

Así, la relación de contenencia en un diagrama de Hasse de *subconjuntos* corresponde (invertida) a la relación de divisibilidad en un diagrama de Hasse de *números*. La matemática, en buena medida, intenta ir descubriendo este tipo de *correlaciones estructurales* entre los objetos, como el estudiante lo irá ampliamente observando a lo largo de su Carrera.

3.2. Cuantificadores

Entendemos aquí por «cuantificadores» los cuantificadores «para todo» y «existe», en su *uso* intuitivo dentro del ámbito de los conjuntos de números y en su uso en las pruebas sencillas del estilo introducido en el capítulo 1. En momentos posteriores de la Carrera de Matemáticas, se realizará tanto un tratamiento axiomático de los cuantificadores (curso de LÓGICA), como un tratamiento *extendido* de los mismos (curso de TEORÍA DE MODELOS), que permiten ampliar la intuición y abrirse a *otros* cuantificadores alternativos, en el mundo de las matemáticas avanzadas.

Los cuantificadores que manejamos a este nivel son:

nombre	*símbolo*	*concepto*	*característica*	*ícono*
cuantificador universal	$\forall$	para todo	cubrir todo	$\otimes$
cuantificador existencial	$\exists$	existe	detectar algo	$\odot$

Las relaciones de inclusión y no inclusión entre conjuntos, que habíamos desbrozado al final del capítulo 1, pueden ahora escribirse de una manera completa gracias a los cuantificadores:

$A \subseteq B$ si y sólo si $\forall a(a \in A \rightarrow a \in B)$

$A \nsubseteq B$ si y sólo si $\exists a(a \in A \wedge a \notin B)$.

Algunas propiedades que habíamos descrito en lenguaje informal podrían ahora codificarse en un pleno lenguaje simbólico, mediante los conectivos y los cuantificadores. Por ejemplo, p es primo se codifica mediante la fórmula $p \in \mathbb{N} \wedge p \geq 2 \wedge \forall n(n \in \mathbb{N} \wedge n \mid p \rightarrow n = 1 \vee n = p)$. Por ejemplo, la caracteri-

zación fundamental de los números primos (ejercicio 1.5) puede codificarse mediante la siguiente fórmula: $\forall n(n \in \mathbb{N} \wedge n \geq 2 \rightarrow (n \text{ es primo } \leftrightarrow \forall a \forall b(a \in \mathbb{N} \wedge b \in \mathbb{N} \wedge n \mid ab \rightarrow n \mid a \vee n \mid b)))$. Por ahora, al nivel bastante intuitivo del curso de FUNDAMENTOS no habrá necesidad de seguir insistiendo en este tipo de codificaciones, aunque se le invita al estudiante a que realice algunas codificaciones por su cuenta. Lo importante es poder contar con la *seguridad de un control bastante razonable de los símbolos*, donde no se mezclen arbitrariamente los objetos de la matemática (como los elementos de los conjuntos de números) con los signos de un lenguaje (como los conectivos y los cuantificadores) construido para hablar sobre esos objetos.

Así como ciertas tautologías nos permitieron codificar y *demostrar* la validez de ciertos razonamientos generales en el ámbito de las matemáticas (como $p \vee \neg p$ codificando el tercio excluso y $(\neg p \rightarrow (q \wedge \neg q)) \rightarrow p$ codificando las pruebas por contradicción), ciertas combinaciones de cuantificadores y conectivos nos permiten codificar algunos razonamientos generales válidos sobre los tránsitos entre lo universal y lo particular. Sin embargo, mientras en el capítulo 2 pudimos introducir adecuados métodos de control y prueba para los conectivos (las tablas de verdad), no podemos aún en esta instancia introducir métodos de control para los cuantificadores. Un curso posterior de LÓGICA remediará estas deficiencias.

Podemos sin embargo señalar algunas leyes válidas para los cuantificadores. Sin poder probarlas por el momento, éstas corresponden no obstante a un entendimiento intuitivo *natural* de los cuantificadores. Sea $P(x)$ una propiedad que se refiere a un cierto universo de elementos matemáticos; tenemos entonces:

$$\neg \forall x P(x) \quad \leftrightarrow \quad \exists x \neg P(x)$$

$$\neg \exists x P(x) \quad \leftrightarrow \quad \forall x \neg P(x)$$

$$\forall x(P(x) \rightarrow Q(x)) \rightarrow (\forall x P(x) \rightarrow \forall x Q(x))$$

$$\exists x(P(x) \wedge Q(x)) \rightarrow (\exists x P(x)) \wedge (\exists x Q(x)).$$

Obsérvese que en la tercera y en la cuarta línea las implicaciones *no* pueden invertirse y que *no* se trata de equivalencias. Por ejemplo, tomando P como la propiedad ser par y Q como la propiedad ser impar, en el universo de los números naturales, para *falsear* la supuesta recíproca de la cuarta línea, basta con observar que existen naturales pares e impares por separado, pero que no existe un natural par e impar a la vez; y para *falsear* la supuesta recíproca de la tercera línea basta con observar que la implicación de la derecha $\forall x P(x) \rightarrow \forall x Q(x)$ es verdadera ya que empieza por una falsedad

(todo natural es par) mientras que la implicación de la izquierda $\forall x(P(x) \rightarrow Q(x))$ es falsa (no todo par es impar).

Teniendo en cuenta los diversos comentarios que hemos hecho en el capítulo, debe entenderse ahora que, cuando nos enfrentamos a conjuntos *infinitos*, en muchos casos va a resultar más fácil ocuparse de los aspectos *negativos* que de los aspectos positivos de esos conjuntos. En efecto, mientras que para mostrar, de manera positiva, una inclusión $A \subseteq B$ habría que chequear que *todo* elemento de A es elemento de B, explorando una lista infinita de elementos de A, o verificando una propiedad en un espectro infinito, procesos que podrían ser muy difíciles de realizar, en cambio, para mostrar, de manera negativa, $A \not\subseteq B$, *bastará con exhibir un elemento* de A que no esté en B.

De esta manera, *en lo que se refiere a contenencias entre conjuntos*, será más fácil tratar el cuantificador existencial, ligado a pruebas negativas, que el cuantificador universal, ligado a pruebas positivas. Con la existencia ($\exists$) podrán *distinguirse* conjuntos mediante contraejemplos. Con la universalidad ($\forall$) deberán en cambio *identificarse* contenencias mediante pruebas generales. Todo esto se resume entonces en el viejo *adagio*, que ha quedado suficientemente sustentado por el momento en este capítulo, según el cual:

un contraejemplo **sí** basta para demostrar una **no** contenencia

un ejemplo **no** basta para demostrar una (**sí**) contenencia.

3.3. Ejercicios

3.1. Demuestre, de dos maneras distintas, que $3\mathbb{Z}$ es infinito: (i) exhibiendo un subconjunto de $3\mathbb{Z}$ «similar» a $\mathbb{N}$; (ii) exhibiendo una parte propia de $3\mathbb{Z}$ «similar» a $3\mathbb{Z}$.

3.2. Demuestre que el conjunto de los números irracionales es infinito, exhibiendo explícitamente una «similitud» entre $\mathbb{N}$ y un *subconjunto* de números irracionales. Ayuda: basta con dar una lista *explícita* infinita de irracionales (recuerde el ejercicio 1.1).

3.3. Considere el conjunto de los números «egipcios» (estudiados con cuidado en el Antiguo Egipto) definido por $\{\frac{1}{q} : q \in \mathbb{N} \wedge q \neq 0\}$. Demuestre, de acuerdo con la definición 3.1, por qué el conjunto de los números egipcios es infinito.

3.4. Complete la tabla siguiente (poniendo en cada casilla $\subseteq$ o $\not\subseteq$, con lectura de izquierda a derecha). Explique con cuidado en cada caso por qué se tiene contenencia (proporcionando una prueba *universal*) o por qué se tiene no contenencia (exhibiendo un contraejemplo *particular*).

$\nearrow$	$\mathbb{N}$	$\mathbb{Z}$	$2\mathbb{Z}$
$3\mathbb{Z}$			
$\mathbb{N}$			
$\{p : p$ es primo $\}$			
$\mathbb{Q}$			

Busque usted, por su cuenta, otras inclusiones o no inclusiones entre los conjuntos infinitos que desee.

3.5. Demuestre que un conjunto finito *no* puede ser similar a una de sus partes propias. Observe la vaguedad del artículo indefinido «un»: puede entenderse como «para todo» conjunto finito (prueba general), o como «para algún» conjunto finito (ejemplo particular). El resultado es válido en cualquier caso. Muéstrelo para un caso particular y demuéstrelo en general.

3.6. Escriba las siguientes frases formalmente, con cuantificadores, e *intente*, en cada caso, demostrar la frase (en un caso ¿cuál? el intento de prueba no podrá completarlo en este curso ¿por qué?).

(i) no todo natural es suma de dos cuadrados

(ii) todo natural es suma de cuatro cuadrados

(iii) no todo natural mayor que 2 es divisible por dos primos distintos

(iv) todo entero diferente de 1 o -1 es divisible por un primo.

3.7. Proporcione ejemplos de propiedades, y de universos donde «encarnen» (es decir, se interpreten) esas propiedades, para los que *no* valga la implicación $\forall a(P(a) \vee Q(a)) \rightarrow (\forall a P(a) \vee \forall a Q(a))$.

3.8. Encuentre una frase formal, con conectivos, cuantificadores, igualdad y *una sola* propiedad binaria $P(x, y)$, que valga en $\mathbb{N}$ con la divisibilidad, y que no valga en $\wp(X)$ con la contenencia (X conjunto arbitrario).

3.9. Encuentre una frase formal, con conectivos, cuantificadores y *una sola* propiedad binaria $P(a, b)$, que valga en $\mathbb{N}$ con el orden usual, y que no valga en $\mathbb{Z}$ con el orden usual.

3.10. ¿Puede usted encontrar una frase formal, con conectivos, cuantificadores y *una sola* propiedad binaria $P(a, b)$, que valga en $\mathbb{Q}$ con el orden usual, y que no valga en $\mathbb{R}$ con ese mismo orden? Inténtelo, pero tal vez unos semestres deberán pasar antes de responder con todo rigor. Descubra por qué el problema parece ser realmente difícil al nivel de un curso de FUNDAMENTOS.

Capítulo 4

Relaciones y funciones

Contenido

4.1. Relaciones 37
4.2. Funciones 42
4.3. Teoremas de Cantor 47
4.4. Ejercicios 50

El mundo de las matemáticas es un mundo orientado hacia la búsqueda de correlaciones entre conceptos. A fines del siglo XIX, con las obras de Peirce y Schröder, se sistematiza la lógica de relaciones, y, con Peano y Russell, las relaciones se integran[1] dentro del panorama conjuntista abierto por Cantor. En la sistematización actual de las matemáticas, las definiciones conjuntistas de relación y función subyacen detrás de todos los demás conceptos.

1 Charles Sanders Peirce (Estados Unidos, 1839-1914), Giuseppe Peano (Italia, 1858-1932) y Bertrand Russell (Inglaterra, 1872-1970) constituyeron una pléyade de brillantes lógicos matemáticos que permitieron asentar firmemente la disciplina. El lugar de Peirce sólo se compara, en la historia de la lógica, con Aristóteles y con Leibniz. La vigencia de la obra de Peano es aún patente en toda nuestra simbología matemática. La influencia de Russell en la «filosofía analítica» cambió el pensamiento en el siglo XX.

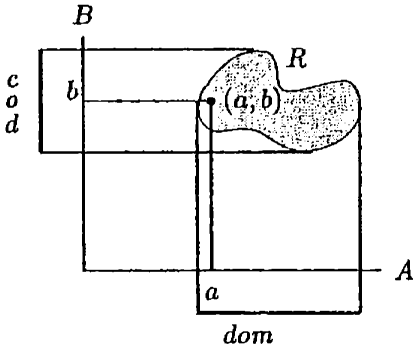
Como el estudiante observará al recorrer el número de ejercicios incluidos, este capítulo es *absolutamente esencial* para una comprensión del curso de FUNDAMENTOS.

4.1. Relaciones

Definición 4.1. Sean A, B dos conjuntos. El **producto (cartesiano)** de A y B es el conjunto de parejas ordenadas $A \times B = \{(a,b) : a \in A \wedge b \in B\}$. Una **relación** R de A en B es un subconjunto de $A \times B$: $R \subseteq A \times B$.

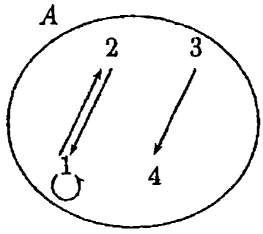
Ejemplo 4.2. Las relaciones recorren ubicuamente el espectro de las matemáticas. Pueden considerarse, por ejemplo, todo tipo de relaciones «triviales» entre conjuntos finitos (conjuntos de parejas al azar), la relación de orden ($\leq$) entre naturales, la relación de divisibilidad ($|$) entre enteros, la relación de inclusión en los conjuntos de partes $\wp(X)$, etc.

Una relación puede verse como una colección de puntos en un plano conceptual:



Definición 4.3. El **dominio** y el **codominio** de una relación $R \subseteq A \times B$ se definen, respectivamente, como el subconjunto de elementos de A relacionados con algún elemento de B, y como el subconjunto de elementos de B relacionados con algún elemento de A. Utilizando los conectivos y los cuantificadores, $dom(R) = \{a : a \in A \wedge \exists b(b \in B \wedge (a,b) \in R)\}$, $cod(R) = \{b : b \in B \wedge \exists a(a \in A \wedge (a,b) \in R)\}$.

En el caso de tener una relación sobre un *mismo* conjunto, y cuando ese conjunto es finito, una relación puede diagramarse cómodamente mediante flechas:



En el diagrama anterior, para el caso $A = \{1,2,3,4\}$, se tiene que $R = \{(1,1),(1,2),(2,1),(3,4)\}$, $dom(R) = \{1,2,3\}$, $cod(R) = \{1,2,4\}$.

Definición 4.4. Sea R una relación sobre un conjunto A ($R \subseteq A \times A$) (A finito o infinito). Para mayor comodidad en la notación, denotamos aRb cada vez que se tenga $(a,b) \in R$. Diremos que:

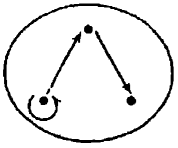
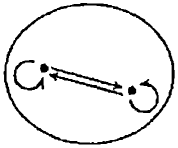
R es **reflexiva** si y sólo si $\forall a(a \in A \rightarrow aRa)$

R es **simétrica** si y sólo si $\forall a \forall b(a,b \in A \wedge aRb \rightarrow bRa)$

R es **transitiva** si y sólo si $\forall a \forall b \forall c(a,b,c \in A \wedge aRb \wedge bRc \rightarrow aRc)$

R es **antisimétrica** si y sólo si $\forall a \forall b(a,b \in A \wedge aRb \wedge bRa \rightarrow a = b)$.

Ejemplo 4.5. En la tabla siguiente pueden observarse algunos ejemplos de relaciones, con sus propiedades respectivas:

relación	*reflexiva*	*simétrica*	*transitiva*	*antisimétrica*
$(\mathbb{N}, <)$	no	no	sí	sí
$(\mathbb{N}, \mid)$	sí	no	sí	sí
$(\wp(A), \subseteq)$	sí	no	sí	sí
$(X, =)$	sí	sí	sí	sí
	no	no	no	sí
	sí	sí	sí	no

Dentro de la inmensa variedad de relaciones que aparecen en matemáticas, dos de los tipos principales son las relaciones de **equivalencia** (relaciones que verifican reflexividad, simetría y transitividad) y las relaciones de **orden** (u «órdenes»: relaciones que verifican reflexividad, antisimetría y transitividad). Tanto las unas como las otras aparecerán incesantemente a lo largo de la Carrera de Matemáticas, las primeras para capturar clases de similitudes entre objetos y estructuras, las segundas para codificar desarrollos y comparabilidades. La igualdad entre los elementos de un conjunto es el arquetipo de una relación de equivalencia; la contenencia entre subconjuntos de un conjunto es el arquetipo de una relación de orden. Como puede observarse en la tabla anterior, la segunda y la tercera líneas corresponden a relaciones de orden, mientras que la cuarta y la sexta líneas corresponden a relaciones de equivalencia.

Sobre las relaciones de equivalencia volveremos repetidamente en los capítulos posteriores (esenciales para la construcción de enteros, racionales y reales: véanse los capítulos 8 y 9, particularmente la sección 8.1). También en los capítulos posteriores estudiaremos los órdenes de naturales (particularmente sección 7.3), enteros, racionales y reales (particularmente, fin de las secciones 8.3 y 9.4), así como el *no orden* de los complejos (fin de la sección 14.1). Los órdenes de los subconjuntos de $\mathbb{R}$ son sin embargo demasiado específicos («órdenes totales» según la definición siguiente), y vale la pena realizar una corta excursión por el abanico de algunos órdenes más generales. Después de la amplia definición siguiente, que cubre múltiples casos que pueden darse dentro de los órdenes, veremos con ejemplos cómo pueden concretarse en la práctica todas las situaciones posibles.

Definición 4.6. Sea R una relación de orden en A (reflexiva, simétrica, transitiva). Denotaremos aRb mediante $a \leq b$, y adoptaremos el lenguaje convencional usual, según el cual a es «menor» que b, y b es «mayor» que a. Sea $a \in A$; a es un elemento **maximal** (para el orden $\leq$) si y sólo si no posee un elemento estrictamente mayor en el orden (con cuidado, esto se expresa en la forma $\forall b \in A(a \leq b \rightarrow b = a)$); similarmente, a es un elemento **minimal** si y sólo si no posee un elemento estrictamente menor en el orden (formalmente, $\forall b \in A(b \leq a \rightarrow b = a)$). Sea ahora $S \subseteq A$, un subconjunto no vacío; S posee un **mínimo** $m = min(S)$ si y sólo si m es un elemento de S menor que todos los demás elementos de S (formalmente, $m \in S$ y $\forall s \in S\ m \leq s$); en forma similar, S posee un **máximo** $m = max(S)$ si y sólo si m es un elemento de S mayor que todos los demás elementos de S (formalmente, $m \in S$ y $\forall s \in S\ s \leq m$). Sea de nuevo $S \subseteq A$ (pero ahora S podría ser vacío), y sea $a \in A$; a es una **cota superior** de S si y sólo si a es mayor que todos

los elementos de S (formalmente, $\forall s \in S\ s \leq a$); similarmente, a es una cota inferior de S si y sólo si a es menor que todos los elementos de S (formalmente, $\forall s \in S\ a \leq s$); S posee un **ínfimo** (denotado $inf(S)$) si y sólo si S posee una máxima cota inferior; similarmente, S posee un **supremo** (denotado $sup(S)$) si y sólo si S posee una mínima cota superior. La relación de orden $\leq$ es un **retículo** si y sólo si todo par de elementos posee un ínfimo y un supremo, es decir, para todos $a, b \in A$ existen $inf(\{a, b\})$ y $sup(\{a, b\})$. La relación de orden $\leq$ es un **orden total** si y sólo si todo par de elementos son comparables en el orden (formalmente, $\forall a, b \in A(a \leq b \ \vee b \leq a)$).

Ejemplo 4.7. Considere la relación de divisibilidad en los naturales (que es un orden según la tabla del ejemplo 4.5). Escogiendo adecuadamente ciertos subconjuntos de naturales, podemos obtener, *dentro* del retículo de divisibilidad de los naturales, las más diversas situaciones de órdenes. Obsérvese ante todo que podríamos ahora eliminar los corchetes alrededor de la expresión «retículo de divisibilidad» si fuésemos capaces de demostrar que existen $inf(\{a, b\})$ y $sup(\{a, b\})$ para el orden de divisibilidad; en realidad, ésto se logra al reemplazar $|$ por $\leq$ en las definiciones, algo que nos lleva inmediatamente a los conceptos de «máximo común divisor» (mcd) y «mínimo común múltiplo» (mcm) (para las definiciones de mcd y mcm, véase el ejemplo 5.4: el manejo de esas definiciones puede realizarse *desde ya*, aunque en ese ejemplo se apliquen para otros cálculos). De hecho, para $a, b \in \mathbb{N}$ y para el orden de divisibilidad, se tiene que $inf(\{a, b\}) = mcd(a, b)$ y $sup(\{a, b\}) = mcm(a, b)$. Sea ahora, por ejemplo, S el conjunto de los divisores de 24; chequee que $min(S) = 1$, $max(S) = 24$, la única cota inferior de S es 1, y existen en cambio infinitas cotas superiores de S (entre las cuales 24, 48, 0); observe también que, *en este caso*, el ínfimo y el supremo de S existen y coinciden respectivamente con mínimo y máximo. Nada en este ejemplo está sin embargo asociado con el número 24; considere por tanto T el conjunto de los divisores de n para un natural n fijo, y chequee que $min(T) = inf(T) = 1$, $max(T) = sup(T) = n$, la única cota inferior de T es 1, y el conjunto de las cotas superiores de S es el conjunto (Infinito) de los múltiplos de n: $\{kn : k \in \mathbb{N}\}$. Sea ahora U el conjunto de las potencias de 2: $U = \{2^k : k \in \mathbb{N}\}$; observe que U no posee máximo (pues dada una potencia de 2, siempre hay otra mayor que ella), pero que, en cambio, U posee supremo: $0 = sup(U)$.

Ejemplo 4.8. El orden de contenencia en $\wp(A)$ (es orden según la tabla del ejemplo 4.5) se ha descrito, para A conjunto finito, en el ejemplo 2.3 y en la discusión subsiguiente a ese ejemplo. Escogiendo ahora adecuadamente ciertos subconjuntos *de subconjuntos* de A, surgen muchas «otras»

situaciones de órdenes (aunque, en realidad, esta supuesta «otredad» no es tal: son sólo «disfraces» de aspectos parciales de la situación anterior, con las *mismas* correlaciones entre los entes, pero con *distintas* «caretas»; véase también, a este propósito, la discusión que precede a la definición 4.13). Sea, por ejemplo, $A = \{1, 2, 3, 4\}$ y sea $S \subseteq \wp(A)$ definido por $S = \{\{2\}, \{3\}, \{2, 3, 4\}\}$; chequee que $min(S) = inf(S) = \{2\}$, $max(S) = sup(S) = \{2, 3, 4\}$, $inf(\{\{2\}, \{3\}\}) = \emptyset \notin S$, $sup(\{\{2\}, \{3\}\}) = \{2, 3\} \notin S$. Observe que S con el orden de contenencia es «esencialmente lo mismo (con distintas caretas)» que el conjunto $\{2, 3, 12\}$ con el orden de divisibilidad (compare, por ejemplo, sus «diagramas de Hasse» respectivos).

De las subdefiniciones incluidas en la definición 4.6, se deducen algunas correlaciones elementales entre los conceptos. Así, la existencia de un mínimo (respectivamente, máximo) fuerza la existencia de un (único) minimal (respectivamente, maximal), mientras que, en cambio, pueden existir múltiples minimales o maximales sin que existan mínimo o máximo. A su vez, si un subconjunto posee un mínimo (respectivamente, máximo) entonces posee ínfimo (respectivamente, supremo), mientras que, en cambio, la existencia del ínfimo (o supremo) no asegura la existencia del mínimo (o máximo), como se vio en el ejemplo 4.7. Por otro lado, todo orden total es inmediatamente un retículo, mientras que no todo retículo es un orden total (y está *muy lejos* de serlo, en general, como lo indica el retículo de divisibilidad de los naturales). Para otras situaciones de órdenes véanse los ejercicios 4.18 y 4.19, así como el ejercicio 10.2 (que puede realizarse desde ya si lo desea el estudiante, pero que se sitúa de forma más natural en el ambiente de los «átomos» conjuntistas del capítulo 10).

Si elaborar una urdimbre sofisticada de relaciones es uno de los objetivos del conocimiento matemático, resulta natural poder contar entonces con operaciones elementales entre relaciones, de tal forma que ciertas relaciones en un nivel dado den lugar a otras nuevas relaciones en un nivel superior. Las dos maneras fundamentales para construir nuevas relaciones, a partir de relaciones dadas, se dan en la siguiente definición.

Definición 4.9. Sea R una relación de A en B ($R \subseteq A \times B$). La **inversa** de R se define por: $R^{-1} = \{(b, a) : (a, b) \in R\}$. Observe que, por definición, $R^{-1} \subseteq B \times A$. Sea R una relación de A en B ($R \subseteq A \times B$), sea S una relación de B en C ($S \subseteq B \times C$). La **compuesta** de R y S se define por: $S \circ R = \{(a, c) : \exists b(aRb \wedge bSc)\}$. Por la definición, se tiene que $S \circ R \subseteq A \times C$. Téngase cuidado con la notación, que *invierte* el orden intuitivo de la composición: primero está R y *luego* S, pero escribimos esa composición

$S \circ R$ *al revés*. Se trata de una notación que puede parecer artificial por el momento, pero que muy pronto resultará natural, al componer *cierto tipo* de relaciones: las funciones.

Ejemplo 4.10. En las tablas siguientes pueden observarse algunos ejemplos de inversas y de compuestas, para casos elementales con conjuntos finitos:

A	B	R	R^{-1}
$\{1,2\}$	$\{3,4,5\}$	$\{(1,3),(2,4)\}$	$\{(3,1),(4,2)\}$
$\emptyset$	$\{1\}$	$\emptyset$	$\emptyset$

A	B	C	R	S	$S \circ R$
$\{1,2\}$	$\{3,4\}$	$\{5,6\}$	$\{(1,3),(2,4)\}$	$\{(3,5),(4,6)\}$	$\{(1,5),(2,6)\}$
$\{1\}$	$\{2,3\}$	$\{4\}$	$\{(1,2)\}$	$\{(3,4)\}$	$\emptyset$
$\emptyset$	$\{2\}$	$\{3\}$	$\emptyset$	$\{(2,3)\}$	$\emptyset$

El dominio y el codominio de las relaciones obtenidas por inversas o por composición están estrechamente conectados con los dominios y codominios de las relaciones originales:

$dom(R^{-1}) = cod(R)$

$cod(R^{-1}) = dom(R)$

$dom(S \circ R) \subseteq dom(R)$

$cod(S \circ R) \subseteq cod(S)$.

Las primeras dos igualdades son inmediatas: por ejemplo, para la primera, si $a \in dom(R^{-1})$ entonces existe b tal que $aR^{-1}b$, es decir bRa, por tanto $a \in cod(R)$. Igualmente, las contenencias tercera y cuarta son consecuencias directas de las definiciones: por ejemplo, para la tercera, si $a \in dom(S \circ R)$ entonces existe c tal que $a(S \circ R)c$, es decir existe b tal que aRb y bSc, pero entonces $a \in dom(R)$. Obsérvese que esas tercera y cuarta contenencias pueden ser *estrictas*: en el segundo ejemplo de la segunda tabla anterior, se observa que $\emptyset = dom(S \circ R) \subsetneq dom(R) = \{1\}$.

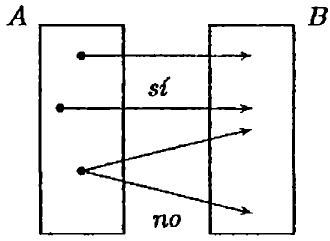
4.2. Funciones

Las funciones son cierto tipo de relaciones en las que se conserva una suerte de *canonicidad simple* en la composición, de tal manera que los elementos correlacionados se sitúan dentro del ámbito de lo *uno* y no dentro del ámbito de lo *múltiple*. Desde comienzos del siglo XIX, toda la matemática moderna

depende en forma *imprescindible* del concepto de función.

Definición 4.11. Sea R una relación de A en B. R es una **función** (de A en B) si y sólo si se cumplen las dos condiciones: (i) $dom(R) = A$ (todo elemento de A está relacionado con *al menos un* elemento de B); (ii) $\forall a(a \in A \wedge aRb \wedge aRc \rightarrow b = c)$ (todo elemento de A está relacionado con *a lo sumo un* elemento de B). Por costumbre de notación, las funciones se denotarán con las letras f, g, etc. Las dos condiciones para una función permiten que se introduzca, *para todo* $a \in A$, el símbolo $f(a)$ para denotar al *único* elemento de B relacionado con a: $f(a)$ se llama la **imagen** de a.

Visualmente, una función debe verse como un diagrama de flechas entre A y B, gobernado por un *permiso* (denotado por un «sí» en el diagrama: sí sale *siempre* una flecha desde todo punto de A) y por una *prohibición* (denotada por un «no» en el diagrama: no salen *nunca* dos flechas desde un mismo punto de A):



Ejemplo 4.12. Algunas funciones interesantes entre conjuntos de números pueden ser las siguientes:

$f : \mathbb{N} \longrightarrow \mathbb{N} : n \mapsto f(n) = n + 1$ («sucesor»)

$g : \mathbb{N} - \{1\} \longrightarrow \mathbb{N} : n \mapsto g(n) =$ mínimo primo que divide a n

$h : \mathbb{Z} \longrightarrow \mathbb{Z} : m \mapsto h(m) = -m$ («inverso aditivo»)

$l : \mathbb{Q} \longrightarrow \mathbb{Q} : \frac{a}{b} \mapsto l(\frac{a}{b}) = \begin{cases} \frac{b}{a}, & a \neq 0; \\ 0, & a = 0. \end{cases}$ («inverso multiplicativo extendido»)

$m : \mathbb{R} \longrightarrow \mathbb{R} : r \mapsto m(r) = r^2$ («cuadrado»)

$n : \mathbb{R} \longrightarrow \mathbb{R} : r \mapsto n(r) = \begin{cases} \sqrt{r}, & \text{si } r \geq 0; \\ 0, & \text{si no.} \end{cases}$ (raíz cuadrada truncada)

Las notaciones estándar (usando $\longrightarrow$ entre conjuntos y $\mapsto$ entre elementos) pueden introducirse gracias a la *unicidad* de las imágenes en las

relaciones que son funciones. Gracias a esa unicidad, pueden también calcularse las compuestas de funciones mediante las aplicaciones sucesivas en las imágenes: $f \circ g(x) = f(g(x))$. Por ejemplo, con las funciones y las notaciones del ejemplo anterior, se tiene que $m \circ n(r) = m(n(r)) = (\sqrt{r})^2 = r$ en el caso $r \geq 0$, mientras que $m \circ n(r) = m(n(r)) = (0)^2 = 0$ en el caso $r < 0$. Por otro lado, $n \circ m(r) = n(m(r)) = \sqrt{(r^2)} = |r|$ (valor absoluto de r) en todos los casos.

Uno de los intereses básicos de las funciones consiste en poder comparar, gracias a ellas, ciertos conjuntos o estructuras. En un primer nivel, como el del curso de FUNDAMENTOS, sólo compararemos los esqueletos de los conjuntos (su «tamaño») y no las posibles estructuras adicionales que éstos puedan tener. Cuando esas estructuras adicionales sirvan para resolver ecuaciones lineales, las funciones habrán de preservar las estructuras propias de lo lineal («espacios vectoriales»): el estudiante se acercará entonces a un curso de ÁLGEBRA LINEAL. Cuando las estructuras sirvan para resolver ecuaciones algebraicas, las funciones habrán de preservar las estructuras propias de lo algebraico («variedades algebraicas»): el estudiante estará entrando a un curso de ÁLGEBRA ABSTRACTA. Cuando las estructuras sirvan para resolver ecuaciones diferenciales, las funciones habrán de preservar las estructuras propias de lo diferencial («variedades diferenciales»): el estudiante se abrirá a un curso de GEOMETRÍA DIFERENCIAL. Cuando las estructuras sirvan para controlar las deformaciones continuas, las funciones habrán de preservar las estructuras propias de lo continuo («espacios topológicos»): el estudiante se adentrará en un curso de TOPOLOGÍA. Y así sucesivamente. Una vez precisadas las diversas problemáticas, así como las estructuras mejor adaptadas para responder a esas problemáticas, muchos de los mayores esfuerzos de los matemáticos consisten luego en estudiar las *transferencias* de conocimiento entre esas diversas estructuras. Toda la matemática del si-

glo XX sigue aquí el legado imperecedero de Galois y Riemann[2], tal vez los dos mayores matemáticos del siglo XIX.

Definición 4.13. Sea f una función de A en B.

f es **1-1** (o inyectiva) si y sólo si toda imagen posee *a lo sumo* una preimagen, es decir, formalmente, $\forall a \forall b(f(a) = f(b) \rightarrow a = b)$.

f es **sobre** (o sobreyectiva) si y sólo si todo elemento del conjunto de llegada posee *al menos* una preimagen, es decir, formalmente, $\forall b(b \in B \rightarrow \exists a \in A\ (b = f(a)))$.

f es **biyección** (o biyectiva) si y sólo si f es a la vez 1-1 y sobre.

Por las definiciones, es fácil chequear que, para una función f, f resulta ser biyectiva si y sólo si la *relación* f^{-1} es función. De hecho, f 1-1 equivale a decir que f^{-1} (como relación) es *funcional* (es decir, que todo elemento de B está relacionado, por medio de f^{-1}, con a lo sumo un elemento de A). Por su lado, f sobre equivale a decir que el dominio de f^{-1} (como relación) cubre todo B (ver ejercicio 4.12). La biyectividad es entonces una propiedad crucial (necesaria y suficiente) para poder *invertir funcionalmente* la mirada: lo que iba de A a B mediante f, lo podríamos mirar de B hacia A mediante la nueva *función* f^{-1}, en el caso de contar con una biyección.

Ejemplo 4.14. Algunas propiedades de las funciones pueden ejemplificarse en la tabla siguiente:

---

[2] Évariste Galois (Francia, 1811-1832) es el paradigma del joven matemático genial. Muerto prematuramente en un duelo por amor, Galois dejó una obra que revolucionó la disciplina, logrando un control cuantitativo de las *ecuaciones algebraicas* mediante un manejo cualitativo de las transferencias y obstrucciones entre *estructuras algebraicas*. Bernhard Riemann (Alemania, 1826-1866) es tal vez el mayor geómetra de todos los tiempos. Riemann consiguió un control cuantitativo de las *ecuaciones diferenciales* mediante un manejo cualitativo de transferencias y obstrucciones entre *espacios topológicos*. El estudio de lo cuantitativo mediante lo cualitativo, en Galois y Riemann, abre un abanico enorme de posibilidades para la matemática.

función	*1-1*	*sobre*	*biyec*
$f : \mathbb{N} \longrightarrow \mathbb{N} : n \mapsto n+7$	sí	no	no
$f : \mathbb{Z} \longrightarrow \mathbb{Z} : m \mapsto m+7$	sí	sí	sí
$f : \mathbb{R} \longrightarrow \mathbb{R} : r \mapsto r^2$	no	no	no
$f : \mathbb{Z} - \{-1, 1\} \longrightarrow \mathbb{Z} : a \mapsto$ mín. primo $p : p \mid a$	no	no	no
$f : \mathbb{Z} \longrightarrow \mathbb{N} : m \mapsto \lvert m \rvert$	no	sí	no

Mediante la noción de biyección se consigue una herramienta muy maleable para poder medir el tamaño de los conjuntos, y para *extender de lo finito a lo infinito* algunos procesos generales de conteo.

Definición 4.15. Sean A y B dos conjuntos. Diremos que A es **similar** a B (o que A es equipotente a B) si y sólo si *existe* una biyección de A en B. Denotaremos por $\sim$ la relación de similaridad entre conjuntos: $A \sim B$ si y sólo si existe una biyección de A en B. Diremos que A y B tienen el **mismo tamaño** (o el mismo **cardinal**) si y sólo si $A \sim B$.

Obsérvese la importancia de la *existencia* de la biyección entre conjuntos similares: basta con *exhibir una* biyección entre dos conjuntos para que sean similares, aunque puedan existir *muchas otras* funciones entre ellos que *no* sean biyecciones. La relación de similaridad entre conjuntos es una crucial *relación de equivalencia*:

Reflexividad: para todo conjunto A, $A \sim A$ mediante la función (biyección) **identidad**: $id_A : A \longrightarrow A : a \mapsto a$.

Simetría: para todos los conjuntos A y B, si $A \sim B$ (mediante una biyección f) entonces $B \sim A$ (mediante la biyección f^{-1}).

Transitividad: para todos los conjuntos A, B y C, si $A \sim B$ (mediante una biyección f) y $B \sim C$ (mediante una biyección g), entonces $A \sim C$ (mediante la biyección compuesta $g \circ f$: véase el ejercicio 4.14).

Ejemplo 4.16. Es fácil demostrar que, aunque $\mathbb{Z}$ *parece* ser el doble de grande que $\mathbb{N}$, y aunque $\mathbb{Z}$ *parece* ser m veces más grande que $m\mathbb{Z}$ (para $m \neq 0$), se tiene en realidad que todos son del *mismo* tamaño:

$$\mathbb{N} \sim \mathbb{Z} \sim m\mathbb{Z} \quad (m \neq 0).$$

En efecto, se puede ver que tenemos $\mathbb{N} \sim \mathbb{Z}$ mediante la biyección (chequearl) $\mathbb{N} \longrightarrow \mathbb{Z} : n \mapsto \begin{cases} \frac{n}{2}, & \text{si } n \text{ es par;} \\ -\frac{n+1}{2}, & \text{si } n \text{ es impar.} \end{cases}$

Por otro lado, es claro que se tiene $\mathbb{Z} \sim m\mathbb{Z}$ (para el caso $m \neq 0$) mediante la biyección «natural» $\mathbb{Z} \longrightarrow m\mathbb{Z} : a \mapsto ma$.

Otro hecho tremendamente importante, pero cuya prueba (o, en realidad, cuyo *camino* de prueba) dejaremos para el capítulo 6, es la similaridad entre naturales y racionales:

$$\mathbb{N} \sim \mathbb{Q}.$$

Se trata, aquí sí, de un hecho tremendamente sorprendente en primera instancia, pues intuitivamente los racionales sobrepasan *infinitamente* a los naturales (no sólo los doblan o los multiplican como en el ejemplo 4.16). Nuestra intuición, educada en un comienzo (colegio, vida cotidiana) en el ámbito de los conjuntos finitos, resulta ser bastante *frágil* en el reino de los conjuntos infinitos. La extensión de esa intuición hacia el ámbito de la infinitud requiere una *educación* y una *experiencia* que sólo la Carrera de Matemáticas puede proveer.

4.3. Teoremas de Cantor

En esta sección demostraremos un par de teoremas de Georg Cantor[3], acerca del *revés* del concepto de similaridad. Cantor se adentra en el mundo de las *diferencias* de tamaño entre los conjuntos, y prueba dos fascinantes *teoremas negativos*: $X \not\sim \wp(X)$ (para *todo* conjunto X), $\mathbb{N} \not\sim \mathbb{R}$. Aquí, $\not\sim$ denota la no similaridad entre los conjuntos, un hecho tremendamente fuerte, ya que *exige* demostrar que *no existe ninguna* biyección posible entre ellos.

Un poco de reflexión indica que no podremos revisar la lista entera de todas las funciones entre un par de conjuntos infinitos y asegurar que ninguna de ellas es una biyección. Al abocarnos a la imposibilidad de recorrer esa lista (así como hubiese sido imposible recorrer la lista de todos los racionales

---

[3] Georg Cantor (Alemania, 1845-1918) es el gran fundador de la teoría de conjuntos, subdisciplina de la matemática que ha servido para reconstruir todas sus demás ramas. La riqueza de las ideas cantorianas (muchas de ellas procedentes de especulaciones filosóficas y teológicas) ha invadido el espectro completo del pensamiento matemático moderno.

para asegurar que $\sqrt{2}$ no aparecía en la lista), hemos entonces de dirigirnos a manejar *pruebas por contradicción.*

Teorema 4.17. *Para todo conjunto* X, $X \not\sim \wp(X)$.

Demostración. Procedemos por contradicción. Suponga que $X \sim \wp(X)$ mediante una cierta biyección f. Para todo $x \in X$, $f(x)$ es entonces un elemento de $\wp(X)$, es decir un subconjunto de X. Tiene así sentido comparar, mediante la relación de pertenencia, el elemento x y el subconjunto $f(x)$. Sea $A = \{x \in X : x \notin f(x)\}$. Por definición, $A \subseteq X$, por tanto $A \in \wp(X)$. *Como f es biyectiva*, en particular es sobreyectiva, y existe $a \in X$ tal que $A = f(a)$. Preguntémonos ahora cómo se comparan a y A con respecto a la relación de pertenencia, y llegaremos a una contradicción (del tipo $p \leftrightarrow \neg p$):

$$a \in A \leftrightarrow a \in f(a) \leftrightarrow \text{no } a \notin f(a) \leftrightarrow \text{no } a \in A \leftrightarrow a \notin A.$$

La primera equivalencia se debe a $A = f(a)$, la segunda se debe a la equivalencia proposicional $\neg\neg p \leftrightarrow p$, la tercera se debe a la definición de la pertenencia en A (que consiste en satisfacer la fórmula $a \notin f(a)$, la cual define intensionalmente a los elementos de A), la cuarta es una notación.

□

La prueba anterior del teorema de Cantor involucra un argumento fundamental de *autorreferencia*, al hacer aparecer ciertos elementos que no pertenecen a una imagen de *sí mismos*. Detrás de esta prueba se esconde un proceso de *diagonalización* muy general, subyacente a muchas *pruebas de imposibilidad* en matemáticas. Es algo que el estudiante querrá tal vez explorar en cursos posteriores de la Carrera (TEORÍA DE CONJUNTOS, TEORÍA DE CATEGORÍAS). Los famosos teoremas de incompletitud de Gödel[4] (tan citados como poco conocidos) pueden verse como casos particulares de

[4] Kurt Gödel (Austria, 1906-1978) es considerado como el mayor lógico matemático del siglo XX (a no confundir con el mayor matemático del siglo XX, título que podrían tal vez disputarse David Hilbert (Alemania, 1862-1943) o Alexander Grothendieck (Francia, n. 1928)). La obra de Gödel explora con suma fineza técnica los linderos del *no* en diversos subespacios de la lógica matemática: aritmética, problemática del continuo, lógicas intuicionista y modal.

argumentos diagonales, que involucran representaciones técnicas de la *paradoja del mentiroso*: la frase «yo miento» lleva a la inescapable contradicción de que miento y digo la verdad a la vez.

El segundo de los teoremas de Cantor que mencionábamos en esta sección es también una forma de argumento diagonal, que en este caso puede exhibirse de manera explícita.

Teorema 4.18. $\mathbb{N} \not\sim \mathbb{R}$.

Demostración. Podemos primero observar intuitivamente (aunque nuestra intuición podría confundirnos) que basta con probar $\mathbb{N} \not\sim [0,1] = \{r \in \mathbb{R} : 0 \leq r \leq 1\}$. En efecto, si con los naturales no somos capaces de cubrir sobreyectivamente todo el intervalo $[0,1]$, menos aún seremos capaces de cubrir sobreyectivamente toda la recta $\mathbb{R}$. Para probar $\mathbb{N} \not\sim [0,1]$ procedemos entonces, de nuevo, por contradicción. Suponga que $\mathbb{N} \sim [0,1]$, es decir que existe una biyección entre los naturales y los reales entre 0 y 1: $\mathbb{N} \longrightarrow [0,1] : n \mapsto r_n$. Esto quiere decir que esos números reales pueden ponerse en una lista (subindicada por los naturales) $r_0, r_1, r_2, \ldots, r_n, \ldots$ Si escribimos la expansión decimal de cada uno de esos reales, tendríamos una situación como la siguiente (asumiendo, sin pérdida de generalidad, que $r_0 = 0$):

$$
\begin{aligned}
r_0 &= 0 \\
r_1 &= 0, r_{11} r_{12} r_{13} \ldots r_{1n} \ldots \\
r_2 &= 0, r_{21} r_{22} r_{23} \ldots r_{2n} \ldots \\
r_3 &= 0, r_{31} r_{32} r_{33} \ldots r_{3n} \ldots \\
&\vdots \\
r_n &= 0, r_{n1} r_{n2} r_{n3} \ldots r_{nn} \ldots
\end{aligned}
$$

(donde todos los r_{ij} son naturales entre 0 y 9: cifras en expansiones decimales).

Afirmamos ahora que esta construcción que *pretendemos* es sobreyectiva, en realidad *no puede serlo*. En efecto, mostremos que existe un número real entre 0 y 1 *diferente de todos los* r_n. Ésta será la *contradicción* deseada, puesto que habíamos supuesto que la lista de los r_n cubría sobreyectivamente todo $[0,1]$. Considere entonces el siguiente número:

$$r = 0, (r_{11} + 1)(r_{22} + 1)(r_{33} + 1) \ldots (r_{nn} + 1) \ldots$$

donde definimos $r_{ii} + 1 = 1$ en caso de que $r_{ii} = 9$ (tomando en los demás casos la suma natural).

Por la construcción misma, se tiene que $r \in [0, 1]$, pero $r \neq r_n$ *para todos* los r_n: basta con observar que, en la n-ésima cifra de la expansión decimal, r y r_n se distinguen, puesto que la n-ésima cifra de la expansión para r es $r_{nn} + 1 \neq r_{nn}$, mientras que la n-ésima cifra de r_n es r_{nn}. □

El número r se construye *modificando la diagonal* en la matriz de las representaciones decimales. El argumento central en la demostración anterior se llama por tanto el **argumento diagonal de Cantor**. Por razones de tipografía, la diagonal puede observarse claramente en el diagrama de las expansiones decimales desplegadas en la página anterior.

4.4. Ejercicios

4.1. Compruebe las propiedades de las relaciones que han sido exhibidas en el ejemplo 4.5.

4.2. Proporcione ejemplos de relaciones R, S, T, tales que: R es transitiva, no simétrica, reflexiva; S es no transitiva, reflexiva; T es simétrica, no transitiva. No confunda la propiedad no simétrica con antisimétrica.

4.3. Sea R una relación sobre X. Sea $\triangle_X$ la relación diagonal en X: $\triangle_X = \{(x, x) : x \in X\}$. Demuestre:

R reflexiva $\leftrightarrow$ $R \supseteq \triangle_X$

R simétrica $\leftrightarrow$ $R = R^{-1}$

R transitiva $\leftrightarrow$ $R \circ R \subseteq R$.

4.4. (i) Sea R la relación en $\mathbb{N}$ definida por aRb si y sólo si $a + b = ab$. Describa R extensionalmente, listando explícitamente todos sus elementos. ¿Es R reflexiva, simétrica, transitiva? Argumente sus respuestas.

(ii) Sea S la relación en $\mathbb{Z}$ definida por aSb si y sólo si $mcd(a, b) = 1$ (donde mcd es el máximo común divisor). ¿Puede usted describir S extensionalmente, listando explícitamente sus elementos? ¿Es S reflexiva, simétrica, transitiva? Argumente sus respuestas.

4.5. Demuestre, para *todas* las relaciones R y S:

$R \subseteq S \leftrightarrow R^{-1} \subseteq S^{-1}$

$R \subseteq S \rightarrow dom(R) \subseteq dom(S)$.

Muestre que la segunda implicación no es una equivalencia.

4.6. Muestre que, en general, $A \times B \neq B \times A$ y que $\wp(A \times B) \neq \wp(A) \times \wp(B)$. ¿Puede determinar algunos casos en los que sí valgan las igualdades?

4.7. A cada real r le asociamos otro real $f(r)$ definido por la ecuación $r^2 + f(r)^2 = 1$. ¿Es esta correspondencia una función de $\mathbb{R}$ en $\mathbb{R}$? A cada racional q le asociamos un real $f(q)$ definido por la ecuación $q^2 + 3f(q) = \sqrt{2}$. ¿Es esta correspondencia una función de $\mathbb{Q}$ en $\mathbb{R}$?

4.8. Muestre que $\emptyset$ no es una función de X en A si el conjunto X no es vacío. Sin embargo, pruebe que $\emptyset$ es una función de $\emptyset$ en A para todo conjunto A.

4.9. Sea $[0,1]$ el intervalo de reales entre 0 y 1. Sea f la función de $[0,1]$ en $\mathbb{Q}$ definida por $f(r) = \begin{cases} 0, & \text{si } r \text{ es irracional;} \\ \frac{1}{q}, & \text{si } r = \frac{p}{q} \text{ con } \frac{p}{q} \text{ fracción irreducible.} \end{cases}$

Calcule $f \circ f$ (ayuda: observe que $f(0) = f(\frac{0}{1}) = 1$).

4.10. Compruebe las propiedades de las funciones exhibidas en la tabla del ejemplo 4.14. Construya usted mismo otros ejemplos concretos de funciones y revise sus propiedades básicas (1-1, sobre, biyección).

4.11. Convénzase de que las definiciones de inyectividad y de sobreyectividad *dependen completamente* de la explicitación del dominio y el codominio de las funciones, y no de la correspondencia escogida. Dicho de otra manera, muestre, por ejemplo, que la correspondencia $x \mapsto x^2$ entre un conjunto de números A y otro conjunto de números B puede ser, dependiendo de cuáles A y B usted especifique, (i) 1-1 y sobre; (ii) 1-1 y no sobre; (iii) no 1-1 y sobre; (iv) no 1-1 y no sobre.

4.12. Sea f una función de A en B. Demuestre que f es 1-1 si y sólo si f^{-1} (entendida como relación) es *funcional*: $(\forall b, a, a')(bf^{-1}a \wedge bf^{-1}a' \rightarrow a = a')$. Aprovechando que $dom(f^{-1}) = cod(f)$ muestre que todo elemento de B posee una imagen por medio de f^{-1} si y sólo si f es sobre. Concluya de todo lo anterior que f es biyectiva si y sólo si f^{-1} es función.

4.13. Chequee que la función propuesta en el ejemplo 4.16 es efectivamente una biyección entre $\mathbb{N}$ y $\mathbb{Z}$. Encuentre al menos otras dos biyecciones diferentes entre $\mathbb{N}$ y $\mathbb{Z}$. ¿Cuántas biyecciones habrá entre esos conjuntos?

4.14. Demuestre que la compuesta de funciones inyectivas es inyectiva y que la compuesta de funciones sobreyectivas es sobreyectiva. Deduzca que la compuesta de biyecciones es biyección. Demuestre que si $f \circ g$ es inyectiva entonces g es inyectiva; con ejemplos, muestre que nada se puede asegurar acerca de la inyectividad de f. Demuestre que si $f \circ g$ es sobreyectiva entonces f es sobreyectiva; con ejemplos, muestre que nada se puede asegurar acerca de la sobreyectividad de g.

4.15. Sea f una función de A en B. Demuestre que, en el caso $A \neq \emptyset$, f es inyectiva si y sólo si existe una función g de B en A tal que $g \circ f = id_A$ (función identidad de A). ¿Qué sucede si $A = \emptyset$? Demuestre que f es sobreyectiva si y sólo si existe una función h de B en A tal que $f \circ h = id_B$ (función identidad de B). Ayuda: dada f, exhiba explícitamente g; no podrá exhibir explícitamente h pero ayúdese de algún principio que le permita escoger elementos de conjuntos no vacíos (aquí se encuentra escondido un axioma complejo de la teoría de conjuntos, el *axioma de elección*, pero proceda por ahora intuitivamente). g se llama la *inversa a izquierda* de f; h se llama la *inversa a derecha* de f.

4.16. Muestre que, para todo conjunto X, no existen inyecciones de $\wp(X)$ en X. Ayuda: proceda por contradicción; a partir de una inyección $f : \wp(X) \longrightarrow X$, considere la *relación* inversa $f^{-1} : X \longrightarrow \wp(X)$ y complétela para dar lugar a una función sobreyectiva entre X y $\wp(X)$, en contradicción con el teorema de Cantor.

4.17. Para todo conjunto X, demuestre que existe una biyección entre el conjunto de partes $\wp(X)$ y el conjunto 2^X, definido como el conjunto de funciones de X en $\{0,1\}$, es decir, $2^X = \{f : X \longrightarrow \{0,1\} : f \text{ es función}\}$. Ayuda: para $S \subseteq X$, sea $f_S \in 2^X$ la función definida por $f_S(x) = 1 \leftrightarrow x \in S$; demuestre entonces que la correspondencia $\wp(X) \longrightarrow 2^X : S \mapsto f_S$ es una biyección. Esto muestra que hay tantos subconjuntos de X como funciones de X en $\{0,1\}$, para cualquier conjunto X (finito o infinito). Para un caso particular de esta situación, vea el ejercicio 10.3.

4.18. Escoja, a su gusto, cinco subdiagramas (apropiadamente distintos en sus formas) del «diagrama de Hasse» correspondiente al retículo de divisibilidad de los naturales, y estudie, para cada uno de ellos, y para adecuados elementos y subconjuntos de esos diagramas, la aparición (o ausencia) de minimales, maximales, mínimos, máximos, cotas superiores, cotas inferiores, ínfimos y supremos. Con este sencillo ejercicio se cubren, *de lejos*, todas las diversas situaciones que el estudiante requiere para entender esos conceptos en situaciones «discretas». Otro uso de los supremos aparecerá de

manera esencial (y radicalmente distinta) en la construcción de los números reales (ver sección 9.4).

4.19. Exhiba ejemplos de conjuntos con relaciones de orden donde se tenga:

(i) tres minimales, un maximal, sin mínimo, sin máximo

(ii) un mínimo, tres maximales, sin máximo

(ii) ningún minimal, ningún maximal.

Capítulo 5

Operaciones entre conjuntos

Contenido

5.1. Complemento, unión, intersección, partes 55
5.2. Imágenes directa e inversa 57
5.3. Ejercicios 60

Partiendo del conjunto vacío, el universo de conjuntos puede expandirse mediante la operación «partes de» (capítulo 3) y mediante otras operaciones, a menudo encontradas en la educación escolar, aunque aquí las introducimos de nuevo sin conocimientos previos: complemento, unión, intersección. Se trata de operaciones que corresponden a manejos proposicionales elementales, ligados, respectivamente, a la negación, la disyunción y la conjunción. Mediante esas operaciones (llamadas operaciones «booleanas», en homenaje al lógico inglés George Boole[1], quien sistematizó su estudio), la urdimbre de los conjuntos adquiere una adecuada «densidad» para poder representar un buen número de objetos de la práctica matemática. En este capítulo estudiamos esas operaciones, así como los (buenos o malos) comportamientos de las funciones con respecto a esas operaciones.

1 George Boole (Inglaterra, 1815-1864) es considerado el padre de la lógica matemática moderna. Boole introdujo herramientas matemáticas (cálculo diferencial, razonamientos algebraicos) en un dominio del saber (el análisis de la razón) que parecía estar destinado a especulaciones lingüísticas o psicológicas.

5.1. Complemento, unión, intersección, partes

Definición 5.1. Sean A y B dos conjuntos. Definimos:

(i) **complemento:** $A^c = \{x : x \notin A\} = \{x : \neg\, x \in A\}$

(ii) **unión:** $A \cup B = \{x : x \in A \vee x \in B\}$

(iii) **intersección:** $A \cap B = \{x : x \in A \wedge x \in B\}$.

Obsérvese cómo cada uno de estos nuevos conjuntos, construidos *a partir* de los anteriores, dependen directamente de los conectivos: conjunto complemento definido a partir del conector $\neg$, conjunto unión definido a partir de $\vee$, conjunto intersección definido a partir de $\wedge$. Usualmente, se desea que cada uno de estos nuevos conjuntos «viva» dentro de un universo dado (tomando, por ejemplo, uniones de subconjuntos de múltiplos en $\mathbb{Z}$, o intersecciones de subconjuntos en $\mathbb{N}$, o complementos de subconjuntos en $\mathbb{R}$, etc.). La noción de complemento presentada en la definición 5.1. puede llevar a problemas (excesivo tamaño en la teoría de conjuntos) si no se la restringe a universos acotados (como $\mathbb{N}$, $\mathbb{Z}$ o $\mathbb{R}$ en los ejemplos anteriores), pero no nos preocuparemos por el momento por esas cuestiones (a debatirse en un curso posterior de TEORÍA DE CONJUNTOS).

Ejemplo 5.2. En la tabla siguiente pueden observarse algunos ejemplos de uniones, intersecciones y complementos, para casos elementales. Denotamos por $\mathbb{I}$ el conjunto de los irracionales.

universo	A	B	$A \cup B$	$A \cap B$	A^c
$\{1,2,3,4\}$	$\{1,2\}$	$\{2,3\}$	$\{1,2,3\}$	$\{2\}$	$\{3,4\}$
$\{1,2,3\}$	$\{1\}$	$\{2\}$	$\{1,2\}$	$\emptyset$	$\{2,3\}$
$\mathbb{N}$	$2\mathbb{N}$	$4\mathbb{N}$	$2\mathbb{N}$	$4\mathbb{N}$	$\{impares\}$
$\mathbb{R}$	$\mathbb{Q}$	$\mathbb{I}$	$\mathbb{R}$	$\emptyset$	$\mathbb{I}$

Ejemplo 5.3. Si *fijamos* un conjunto A como universo dado, y observamos el conjunto $\wp(A)$ de sus subconjuntos, las operaciones unión, intersección y complemento actúan *dentro de* $\wp(A)$ de manera natural, definiendo en cada caso nuevos subconjuntos de A. Combinando las diversas informaciones que se tienen (o que pueden demostrarse: ejercicio 5.1), se descubre una muy rica *estructura* $(\wp(A), \cap, \cup, ()^c, \emptyset, A, \subseteq)$ donde valen muchas relaciones entre los subconjuntos de A. De hecho, para todos X, Y, $Z \subseteq A$:

- $\emptyset \subseteq X$ ($\emptyset$ es un *mínimo* para la contenencia)

- $X \subseteq A$ (A es un *máximo* para la contenencia)
- $X \cap X^c = \emptyset$, $X \cup X^c = A$ (leyes de complementariedad)
- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

  $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ (leyes de distributividad)

Las estructuras con operaciones y propiedades similares a las anteriores se llaman «álgebras de Boole». Estas álgebras aparecen ubicuamente en el espectro de las matemáticas, como el estudiante tendrá la oportunidad de comprobarlo en su Carrera. El mundo de los posibles se abrirá cuando el estudiante descubra que *no* todas las álgebras de Boole pueden representarse sin embargo como álgebras de subconjuntos (del tipo $\wp(A)$ para algún conjunto A). El curso de TOPOLOGÍA le abrirá entonces al matemático nuevas y fantásticas compuertas de acceso al infinito.

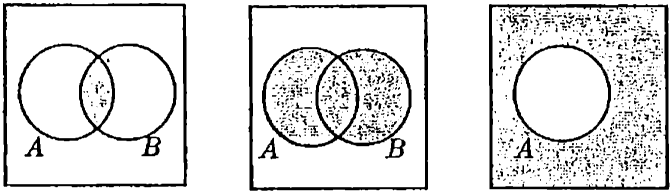
Ejemplo 5.4. Sean m y n naturales. Entonces $m\mathbb{Z} \cap n\mathbb{Z} = mcm(m,n)\mathbb{Z}$, donde $mcm(m,n)$ denota el **mínimo común múltiplo** de m y n (por definición, $r = mcm(m,n)$ si y sólo si (i) $m \mid r$ y $n \mid r$ (ii) r es el *mínimo* número con esa propiedad: si $m \mid r'$ y $n \mid r'$ entonces $r \mid r'$). Demostremos, en efecto, que los dos conjuntos son iguales, mostrando que cada uno está incluido en el otro. Para ver $m\mathbb{Z} \cap n\mathbb{Z} \subseteq mcm(m,n)\mathbb{Z}$, sea $x \in m\mathbb{Z} \cap n\mathbb{Z}$: eso significa que x es múltiplo de m y de n a la vez, por tanto es múltiplo de su mínimo común múltiplo (propiedad (ii)), es decir $x \in mcm(m,n)\mathbb{Z}$. Por otro lado, para ver $mcm(m,n)\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$, sea $x \in mcm(m,n)\mathbb{Z}$: entonces (propiedad (i)) $m \mid mcm(m,n) \mid x$ implica $x \in m\mathbb{Z}$, y $n \mid mcm(m,n) \mid x$ implica $x \in n\mathbb{Z}$, por tanto $x \in m\mathbb{Z} \cap n\mathbb{Z}$.

Por otro lado, *no* se tiene $m\mathbb{Z} \cup n\mathbb{Z} = mcd(m,n)\mathbb{Z}$, como tal vez podría intuirse en una primera aproximación «dialéctica», en un movimiento «pendular entre el «y» y el «o», entre el mínimo común múltiplo y su «contraparte», el **máximo común divisor** $mcd(m,n)$ (por definición, $d = mcd(m,n)$ si y sólo si (i) $d \mid m$ y $d \mid n$ (ii) d es el *máximo* número con esa propiedad: si $d' \mid m$ y $d' \mid n$ entonces $d' \mid d$). De hecho, $2\mathbb{Z} \cup 3\mathbb{Z}$ es el subconjunto de los enteros que son múltiplos de 2 o de 3, y 7 no aparece, por ejemplo, en esa lista; sin embargo, $mcd(2,3) = 1$ y por tanto $mcd(2,3)\mathbb{Z} = \mathbb{Z}$ que contiene al 7. En general, se tiene $m\mathbb{Z} \cup n\mathbb{Z} \subseteq mcd(m,n)\mathbb{Z}$, pero en la mayoría de los casos la inclusión será *estricta*.

Aunque las uniones e intersecciones están ligadas a conectivos, y, como acabamos de ver en el caso aritmético, a números distinguidos como el *mcm* y el *mcd*, *en cambio* la definición del conjunto de partes (ver ejem-

plo 2.3) *no* está asociada a ningún conectivo. El teorema de Cantor (4.14) muestra que $\wp(X)$ crece mucho más rápido que X, para todo conjunto X (algo que habíamos chequeado, en el caso finito, en el ejemplo 2.3). En realidad, la operación partes de, aplicada a conjuntos infinitos, puede llegar a ser tremendamente compleja, y en ciertos casos casi indescifrable, como lo indicamos en el capítulo 10.

Las operaciones de intersección, unión y complemento pueden visualizarse de manera cómoda gracias a los conocidos **diagramas de Venn**[2]:



Las regiones delineadas representan, de izquierda a derecha, $A \cap B$, $A \cup B$ y A^c (en el *universo* rectangular dado). No obstante, estas representaciones cómodas pueden ser imposibles de diagramar para conjuntos infinitos. Las imágenes obtenidas con los diagramas de Venn sirven de ayuda, y pueden ser una buena guía, pero deben ser luego controladas mediante los instrumentarios propios que ayudan a calibrar el infinito: cuantificadores, relaciones, funciones.

5.2. Imágenes directa e inversa

Las operaciones conjuntistas usuales, que hemos visto en la sección anterior, tienden a concentrarse en un universo fijo, en el cual se realizan los cálculos. El espacio de las matemáticas es sin embargo variable, y en su variabilidad radica en buena medida su riqueza. Al poner en correspondencia dos universos, es decir, en los casos usuales, al tener ciertas funciones entre colecciones

---

2 John Venn (Inglaterra, 1834-1923) forma parte de una brillante escuela inglesa de lógicos matemáticos, que continuaron desarrollando la disciplina después de los aportes precursores de Boole.

de subconjuntos, resulta importante saber en qué medida se preservan las operaciones de cada universo.

Definición 5.5. Sea f una función entre A y B. Definimos:

(i) **imagen directa:** $\overrightarrow{f}(X) = \{f(x) : x \in X\}$, para $X \subseteq A$

(ii) **imagen inversa:** $\overleftarrow{f}(Y) = \{x : f(x) \in Y\}$, para $Y \subseteq B$.

En la definición anterior, f puede ser *cualquier* función: no se requiere que sea ni 1-1, ni sobre. Observe que, por la definición, para $X \subseteq A$, $\overrightarrow{f}(X) \subseteq cod(f)$, por tanto $\overrightarrow{f}(X) \subseteq B$ (ya que $cod(f) \subseteq B$). De manera similar, para $Y \subseteq B$ se tiene siempre $\overleftarrow{f}(Y) \subseteq dom(f) = A$. Dada una función f, que envía elementos en elementos, las imágenes directa e inversa envían en cambio *subconjuntos en subconjuntos*. No deben confundirse aquí los objetos sobre los cuales se trabaja.

Dada f función de A en B, las imágenes directa e inversa son por tanto dos nuevas funciones entre los conjuntos de partes $\wp(A)$ y $\wp(B)$ ($\overrightarrow{f}$ y $\overleftarrow{f}$ son claramente relaciones, demuestre que son funciones!):

$$A \xrightarrow{\ f\ } B$$

$$\wp(A) \xrightarrow{\ \overrightarrow{f}\ } \wp(B)$$

$$\wp(A) \xleftarrow{\ \overleftarrow{f}\ } \wp(B)$$

Ejemplo 5.6. La tabla siguiente exhibe algunos cálculos de imágenes directas e inversas para ejemplos sencillos (donde $X \subseteq A$ y $Y \subseteq B$):

A	B	f	X	$\overrightarrow{f}(X)$	Y	$\overleftarrow{f}(Y)$
$\{1,2\}$	$\{3,4\}$	$n \mapsto n+2$	$\{1\}$	$\{3\}$	$\{4\}$	$\{2\}$
$\mathbb{N}$	$\mathbb{N}$	$n \mapsto n+1$	$2\mathbb{N}$	$\{impares\}$	$\{0\}$	$\emptyset$
$\mathbb{N}$	$\mathbb{N}$	$n \mapsto 6n$	$\{p\}$	$\{6p\}$	$\{primos\}$	$\emptyset$
$\mathbb{Q}$	$\mathbb{R}$	$q \mapsto \sqrt{\lvert q \rvert}$	$\emptyset$	$\emptyset$	$\{\sqrt{3}\}$	$\{-3,3\}$

La imagen inversa siempre se comporta bien con respecto a las operaciones conjuntistas usuales. Si f es una función de A en B y Y, Y_1, Y_2 son subconjuntos de B, tenemos:

- $\overleftarrow{f}(Y_1 \cup Y_2) = \overleftarrow{f}(Y_1) \cup \overleftarrow{f}(Y_2)$
- $\overleftarrow{f}(Y_1 \cap Y_2) = \overleftarrow{f}(Y_1) \cap \overleftarrow{f}(Y_2)$
- $\overleftarrow{f}(Y^c) = (\overleftarrow{f}(Y))^c$

En efecto, para la primera igualdad, $x \in \overleftarrow{f}(Y_1 \cup Y_2) \leftrightarrow f(x) \in Y_1 \cup Y_2 \leftrightarrow f(x) \in Y_1 \vee f(x) \in Y_2 \leftrightarrow x \in \overleftarrow{f}(Y_1) \vee x \in \overleftarrow{f}(Y_2) \leftrightarrow x \in \overleftarrow{f}(Y_1) \cup \overleftarrow{f}(Y_2)$. La segunda igualdad se obtiene de manera similar, reemplazando en la prueba unión por intersección, y disyunción por conjunción (compruébelo!). Para la tercera igualdad, $x \in \overleftarrow{f}(Y^c) \leftrightarrow f(x) \in Y^c \leftrightarrow f(x) \notin Y \leftrightarrow \neg f(x) \in Y \leftrightarrow \neg x \in \overleftarrow{f}(Y) \leftrightarrow x \in (\overleftarrow{f}(Y))^c$. Obsérvese cómo, en estas pruebas, sólo se usan las definiciones, sin requerir *absolutamente nada más*. Esto muestra que la definición de imagen inversa es particularmente apropiada para capturar de manera *intrínseca* el *buen tránsito* entre las operaciones booleanas.

El magnífico comportamiento de la imagen inversa *no* se contagia a la imagen directa. De hecho, aunque la imagen directa preserva uniones (para X_1 y X_2 subconjuntos de A):

- $\overrightarrow{f}(X_1 \cup X_2) = \overrightarrow{f}(X_1) \cup \overrightarrow{f}(X_2)$

la imagen directa no preserva en cambio, en general, ni la intersección, ni el complemento. Tomando, por ejemplo, la función $f : \mathbb{Z} \longrightarrow \mathbb{Z} : m \mapsto m^2$, y tomando $X_1 = \{m : m \leq 0\}$, $X_2 = \{m : m \geq 0\}$, se tiene que $X_1 \cap X_2 = \{0\}$, por tanto $\overrightarrow{f}(X_1 \cap X_2) = f(\{0\}) = \{0\}$, mientras que $f(X_1) = f(X_2) = f(X_1) \cap f(X_2)$, todos iguales al subconjunto de los números cuadrados, un subconjunto mucho más grande que $\{0\}$. Por otro lado, si se toma por ejemplo la función $f : \mathbb{Z} \longrightarrow \mathbb{N} : m \mapsto |m|$ (valor absoluto) y se toma $X = \{m : m \leq 0\}$, se tiene que $\overrightarrow{f}(X) = \mathbb{N}$, por tanto $(\overrightarrow{f}(X))^c = \emptyset$ (tomamos complementos en $\mathbb{N}$, el codominio de f), mientras que $X^c = \{m : m > 0\}$ (tomamos aquí complementos en $\mathbb{Z}$, el dominio de f), por tanto $\overrightarrow{f}(X^c) = \{m : m > 0\}$, un conjunto de nuevo mucho más grande.

Puede mostrarse (hágalo!) que siempre vale en general la contenencia $\overrightarrow{f}(X_1 \cap X_2) \subseteq \overrightarrow{f}(X_1) \cap \overrightarrow{f}(X_2)$, aunque ésta, como acabamos de ver, puede ser estricta. De hecho (ver ejercicio 5.8), la inclusión podrá ser siempre estricta si la función f no es 1-1. Por otro lado, para los complementos, ninguna de las dos inclusiones vale en general; de hecho, $(\overrightarrow{f}(X))^c \subseteq \overrightarrow{f}(X^c)$ puede también fallar (considere, por ejemplo, la función $f : \mathbb{Z} \longrightarrow \mathbb{N} : m \mapsto m^2$: para apropiados subconjuntos X falla la inclusión). Sólo en el caso de te-

ner una biyección, la imagen directa se comportará bien con respecto al complemento (ejercicio 5.9).

5.3. Ejercicios

5.1. Demuestre las diversas aserciones anunciadas como labor para el lector y no probadas en el cuerpo del texto: las leyes de complementariedad y distributividad, el hecho de que las imágenes inversa y directa son funciones entre los conjuntos de partes, el hecho de que la imagen directa preserva uniones y el hecho de que la imagen directa de una intersección está contenida en la intersección de las imágenes directas. Verifique la corrección de los casos presentados en el ejemplo 5.6.

5.2. Sean A y B dos conjuntos. Demuestre: $A \subseteq B$ si y sólo si $A \cup B = B$ si y sólo si $A \cap B = A$.

5.3. Sea A un conjunto tal que $A \cup X = X$ para todo conjunto X. Demuestre que $A = \emptyset$.

5.4. Proporcione ejemplos de dos conjuntos A y B tales $\wp(A \cup B) \neq \wp(A) \cup \wp(B)$. ¿Qué cree que sucederá cambiando unión por intersección? Demuestre su aserción.

5.5. Dado un conjunto A, para X y Y subconjuntos de A definimos $X \triangle Y = (X \cap Y^c) \cup (X^c \cap Y)$ (diferencia simétrica de X y Y). Demuestre que $X \triangle X = \emptyset$, $X \triangle \emptyset = X$, $X \triangle Y = Y \triangle X$ (pruebas fáciles). Demuestre también que $(X \triangle Y) \triangle Z = X \triangle (Y \triangle Z)$ (prueba más larga). ¿Vale una ley de distributividad del tipo: $(X \triangle Y) \cup Z = (X \cup Z) \triangle (Y \cup Z)$? Si la respuesta es positiva, provea una prueba general; si la respuesta es negativa, provea un contraejemplo particular.

5.6. Sean A, B y C tres conjuntos. Demuestre que $A \cup C = B \cup C$ no implica $A = B$, pero que, en cambio, $A \triangle C = B \triangle C$ sí implica $A = B$ (donde $\triangle$ es la diferencia simétrica del ejercicio anterior). Con esto, puede usted observar que la unión no actúa como una suma aritmética de conjuntos, y que, en cambio, la diferencia simétrica sí funciona como tal (pues permite *cancelatividad*, como la suma de números).

5.7. Dadas las funciones $f : \mathbb{N} \longrightarrow \mathbb{R} : n \mapsto \sqrt{n}$, $g : \mathbb{Z} - \{-1, 1\} \longrightarrow \mathbb{N} : m \mapsto$ mínimo primo que divide a m, $h : \mathbb{Q} \longrightarrow \mathbb{Q} : q \mapsto q^{-1}$ (si $q \neq 0$), $0 \mapsto 0$, calcule las siguientes imágenes directas e inversas: $\overrightarrow{f}(\{2^n : n \in \mathbb{N} \wedge n \geq 2\})$, $\overrightarrow{g}(\{0, 2, 3, 5, 100, 2310\})$, $\overrightarrow{h}(\mathbb{N})$, $\overleftarrow{f}(\{4, 9, 16, 25\})$, $\overleftarrow{g}(\{0, 11, 14\})$, $\overleftarrow{h}(\mathbb{Z})$.

5.8. Sea f una función de A en B. Demuestre que f es 1-1 si y sólo si para todos X_1 y X_2 subconjuntos de A se tiene $\overrightarrow{f}(X_1 \cap X_2) = \overrightarrow{f}(X_1) \cap \overrightarrow{f}(X_2)$. Ayuda: la contrarrecíproca puede simplificar algunas aserciones a demostrar.

5.9. Sea f una función biyectiva de A en B. Demuestre que para todo X subconjunto de A se tiene $(\overrightarrow{f}(X))^c = \overrightarrow{f}(X^c)$. Deben aquí tomarse complementos en cada uno de los universos apropiados A, B; en rigor, la frase anterior debería escribirse $\overrightarrow{f}(A - X) = B - \overrightarrow{f}(X)$, pero se pierde de vista entonces la lectura elemental de preservar complementos.

Capítulo 6

Tamaños de infinitud

Contenido

6.1. Inyecciones entre conjuntos infinitos 62
6.2. Ejercicios 67

En este capítulo indicamos las principales comparaciones de tamaño entre los conjuntos usuales de números. Recuérdese (definición 4.15) que dos conjuntos tienen el mismo tamaño (o el mismo cardinal) si existe una biyección entre ellos. En el ejemplo 4.16 vimos cómo los conjuntos de naturales, de enteros, y de múltiplos de un entero no nulo, tienen todos el mismo tamaño. Con los teoremas de Cantor (4.17, 4.18), en cambio, vimos cómo los tamaños de los conjuntos de partes *no* son iguales a los tamaños de los conjuntos iniciales, y cómo el tamaño del conjunto de los números reales *no* es igual al tamaño del conjunto de los naturales.

6.1. Inyecciones entre conjuntos infinitos

Es útil poder comparar los tamaños de los conjuntos mediante una relación de «menor tamaño». Se tiene entonces una relación menos exigente que la de similaridad, con la cual es más cómodo proceder en la práctica.

Definición 6.1. Sean A y B dos conjuntos. Decimos que el tamaño de A es **menor** que el tamaño de B (o que el cardinal de A es menor que el cardinal de B) si y sólo si existe una inyección de A en B. Notación: $\overline{\overline{A}} \leq \overline{\overline{B}}$ (donde $\overline{\overline{A}}$ denota el cardinal de A).

Puesto que la compuesta de funciones inyectivas es inyectiva (ejercicio 4.13), resulta que $\overline{\overline{A}} \leq \overline{\overline{B}}$ y $\overline{\overline{B}} \leq \overline{\overline{C}}$ implica $\overline{\overline{A}} \leq \overline{\overline{C}}$: el «crecimiento» de los tamaños se preserva por la relación $\leq$. Un hecho importante en teoría de conjuntos, que *asumiremos en este capítulo sin demostración* (y cuya elucidación queda, por tanto, para un curso posterior de TEORÍA DE CONJUNTOS), es el hecho de que $\leq$ se comporta como una *genuina* relación de *orden* entre cardinales:

Teorema de Schröder-Bernstein.[1] Sean A y B dos conjuntos. Si existe una inyección de A en B y si existe una inyección de B en A, entonces existe una biyección de A en B.

Obsérvese que el interés del teorema radica en que, *a priori*, las dos inyecciones anteriores no tienen por qué ser recíprocas la una de la otra (y, de hecho, en la práctica, a menudo no lo son). Sin embargo, mediante dos inyecciones *cualesquiera*, en sentido inverso la una de la otra, el teorema permite construir *siempre* una biyección. Con las notaciones anteriores, esto se expresa diciendo que $\leq$ es antisimétrica: $\overline{\overline{A}} \leq \overline{\overline{B}}$ y $\overline{\overline{B}} \leq \overline{\overline{A}}$ implica $\overline{\overline{A}} = \overline{\overline{B}}$.

Dos constataciones elementales aseguran que

$$A \subseteq B \text{ implica } \overline{\overline{A}} \leq \overline{\overline{B}}$$

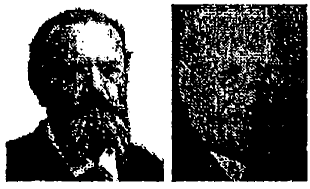
$$\overline{\overline{X}} \leq \overline{\overline{\wp(X)}}.$$

En efecto, si A está contenido en B, la función identidad de A actúa como inyección de A en B. Por otro lado, la función *singleton* $f : X \longrightarrow \wp(X)$ definida por $f(x) = \{x\}$ es claramente una inyección (demuéstrelo!).

En el diagrama siguiente comprimimos toda la información acerca de posibles inyecciones entre los conjuntos de números usuales. En el diagrama, el símbolo $\rightarrow$ denotará «existe una inyección». Sólo indicamos las flechas necesarias para captar la información; de hecho, las *compuestas* de las flechas presentadas dan lugar a otras flechas no presentadas (pues compuesta de

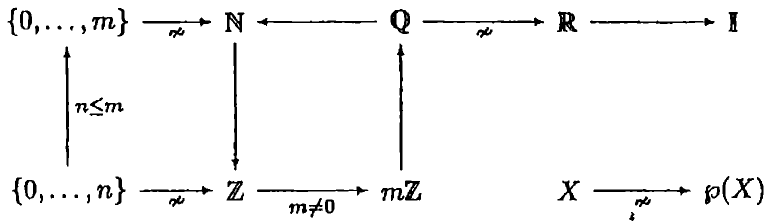
---

1 Ernst Schröder (Alemania, 1841-1902) sistematizó la obra precursora de Peirce en la lógica de las relaciones, y promulgó su entendimiento como base imprescindible del saber matemático moderno. Felix Bernstein (Alemania, 1878-1956) fue uno de los exponentes de la escuela que promovió el uso de la teoría de conjuntos como fundamento último de la matemática.



inyecciones es inyección). Los símbolos $\nrightarrow$ denotan inyecciones para las cuales no existe inyección inversa. Por supuesto, la aparición de un símbolo $\nrightarrow$ es mucho más delicada que la aparición del símbolo $\to$, puesto que requiere asegurar que *ninguna* inyección es posible, en un espectro usualmente infinito de posibilidades.

Universo de inyecciones entre conjuntos



Observemos en detalle cada una de estas posibilidades de inyecciones (o *necesidades* de *no* inyecciones):

(i) Si $n \leq m$, $\{0,\ldots,n\} \subseteq \{0,\ldots,m\}$, por lo tanto el primer conjunto se inyecta en el segundo.

(ii) $\mathbb{N}$ no puede inyectarse en un conjunto finito del tipo $\{0,\ldots,m\}$, pues toda función de $\mathbb{N}$ en $\{0,\ldots,m\}$ tendrá que tener necesariamente repeticiones.

(iii) Ya vimos (ejemplo 4.13) que $\mathbb{N}$, $\mathbb{Z}$ y $m\mathbb{Z}$ (para $m \neq 0$) poseen biyecciones entre ellos; con mayor razón se tienen adecuadas inyecciones.

(iv) La inclusión de $m\mathbb{Z}$ en $\mathbb{Q}$, así como la inclusión de $\mathbb{Q}$ en $\mathbb{R}$, aseguran inyecciones entre ellos.

(v) La función «singleton» entre X y $\wp(X)$ asegura una inyección entre ellos. El teorema de Cantor 4.14 demuestra que no existe biyección entre ellos. Por lo tanto, no existe inyección de $\wp(X)$ en X: en efecto (por contradicción), si existiese una inyección de $\wp(X)$ en X, combinando esa inyección con la inyección de X en $\wp(X)$ podría construirse (por el teorema de Schröder-Bernstein) una biyección entre X y $\wp(X)$, contradiciendo el teorema de Cantor.

(vi) *Existe una inyección entre* $\mathbb{Q}$ y $\mathbb{N}$. Después de los teoremas de Cantor, éste es otro de los comportamientos de los conjuntos infinitos que va en contra de nuestra intuición (finitaria). Sin embargo, con un poco de reflexión, se observa que un racional está esencialmente determinado por dos enteros,

y éstos a su vez por cuatro naturales. No resulta tan extraño pensar entonces en la siguiente función: $f : \mathbb{Q} \longrightarrow \mathbb{N}$

$$\frac{a}{b} \mapsto \begin{cases} 2^a 3^b, & a, b \in \mathbb{N}, b \neq 0\ ; \\ 5^a 7^{-b}, & a \in \mathbb{N}, b \in \mathbb{Z}, b < 0, \end{cases}$$

donde un racional $\frac{a}{b}$ se escribe sin factores comunes y en alguna de las dos formas contempladas en la definición de f. El hecho de escribir los racionales en forma reducida, sin factores comunes, asegura la *funcionalidad* de f (recuérdese, en particular, que 0 se escribe en forma reducida $0 = \frac{0}{1}$, por lo que $f(0) = 2^0 3^1 = 3$). La *inyectividad* de f se deduce de la factorización *única* en números primos (ver ejercicio 1.5): las imágenes bajo f dependen entonces en forma única de a y de b, es decir, f es inyectiva.

(vii) A partir de una inyección $\mathbb{Q} \longrightarrow \mathbb{N}$, como la anterior, y de la inyección obvia $\mathbb{N} \longrightarrow \mathbb{Q}$, se tiene (por Schröder-Bernstein) que los dos conjuntos son similares. Téngase cuidado: asumiendo Schröder-Bernstein, estamos así asegurando que *existe* una biyección entre $\mathbb{Q}$ y $\mathbb{N}$; si se quisiera construir *explícitamente* una tal biyección, el trabajo sería *mucho más difícil* que el realizado en el punto (vi).

(viii) El teorema de Cantor 4.15 nos asegura que $\mathbb{N} \not\sim \mathbb{R}$. Acabamos de ver que $\mathbb{N} \sim \mathbb{Q}$, por lo tanto $\mathbb{Q} \not\sim \mathbb{R}$.

(ix) Una inyección entre $\mathbb{N} \times \mathbb{N}$ y $\mathbb{N}$ puede darse, siguiendo la idea expresada en (vi), por $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} : (n, m) \mapsto 2^n 3^m$. Combinando con la inyección obvia $\mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N} : n \mapsto (n, n)$, el teorema de Schröder-Bernstein asegura que $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ (de nuevo, una biyección explícita no es aquí inmediata). Si A y B son dos conjuntos similares a $\mathbb{N}$, entonces $A \cup B$ es también similar a $\mathbb{N}$: una inyección de $A \cup B$ en $\mathbb{N}$ resulta como compuesta de las inyecciones $A \cup B \subseteq A \sqcup B \longrightarrow \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, con $(a_n, b_m) \mapsto (n, m)$ en la segunda inyección ($A \sqcup B$ es la unión disyunta, y los $(a_n)_{n \geq 0}$ y $(b_m)_{m \geq 0}$ son listas sin repeticiones de los elementos de A y de B).

(x) Si denotamos por $\mathbb{I}$ el conjunto de números irracionales, se tiene que $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. Como $\mathbb{Q} \sim \mathbb{N}$, entonces se tiene $\mathbb{I} \not\sim \mathbb{N}$: si no, por el comentario (ix), la unión $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$ sería similar a $\mathbb{N}$, contradiciendo el teorema diagonal de Cantor (4.15). Para una inyección entre $\mathbb{R}$ e $\mathbb{I}$, véase el ejercicio 6.2.

Definición 6.2. Un conjunto A se dice **enumerable** si es del mismo tamaño que $\mathbb{N}$.

Los resultados anteriores nos aseguran que los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $m\mathbb{Z}$ ($m \neq 0$), $\mathbb{Q}$ son todos enumerables, mientras que los conjuntos $\mathbb{R}$ e $\mathbb{I}$ son no enumerables. Además, si X es enumerable, entonces $\wp(X)$ no es enumerable.

En el infinito, se establece así una primera barrera entre lo enumerable y lo no enumerable. Ahora bien, dentro de lo *no enumerable*, emerge luego una inmensa (infinita) jerarquía de tamaños, con la teoría de los cardinales transfinitos (o *alephs*) de Cantor. El refinamiento de la jerarquía no alcanza a vislumbrarse dentro de los conjuntos elementales de números, pero el *universo de las posibilidades explota* posteriormente en el transfinito cantoriano.

Hemos visto que $m\mathbb{Z} \sim \mathbb{Z}$ si $m \neq 0$, así como, en los comentarios después de la definición 3.1, habíamos visto que el conjunto de los naturales es similar al conjunto de los pares positivos. Se trata de un comportamiento típico de los conjuntos infinitos, que podríamos intentar erigir en una definición alternativa de la infinitud:

Definición 6.3. Un conjunto es **infinito** si y sólo si contiene un subconjunto *propio* equipotente al conjunto *completo*: A es infinito cuando $\exists X \subsetneq A (X \sim A)$. La clave fundamental es que X sea un subconjunto estrictamente contenido en A.

Si los FUNDAMENTOS de la matemática se establecieran sobre bases completamente firmes, las dos definiciones 3.1 y 6.3 deberían ser *equivalentes*. Se trata de una equivalencia que sólo podrá conseguirse de manera completa en un curso posterior de TEORÍA DE CONJUNTOS, pero puede aquí al menos intuirse la *plausibilidad* de la equivalencia.

En efecto, si A es un conjunto infinito en el sentido de la definición 3.1, A contiene un subconjunto X equipotente a $\mathbb{N}$ (la noción de similaridad introducida intuitivamente en 3.1 es ya reemplazada aquí por la biyectividad correspondiente). Sea $X = \{a_0, a_1, a_2, \ldots, a_n, \ldots\}$. Es claro que $X \sim X - \{a_0\}$ (conjunto X excepto a_0), mediante la biyección $f : a_n \mapsto a_{n+1}$. Se deduce entonces $A \sim A - \{a_0\}$, mediante la biyección que consiste en la identidad si $a \notin X$ y en la función f si $a \in X$. Al tener $A \sim A - \{a_0\} \subsetneq A$, A es equipotente a una de sus partes propias (la más sencilla: A excepto un elemento), es decir, A es infinito según la definición 6.3.

Las razones que sustentarían el argumento inverso («infinito» según 6.3 implica «infinito» según 3.1) superan, en cambio, los argumentos que podrían darse al nivel de este primer curso de FUNDAMENTOS. El buen estudiante no querrá sin embargo dejar de explorar las dificultades de la situación.

6.2. Ejercicios

6.1. Encuentre una biyección explícita entre $\mathbb{N} \times \mathbb{N}$ y $\mathbb{N}$ (ya sea dibujándola, ya sea construyendo explícitamente una fórmula).

6.2. Encuentre una inyección entre $\mathbb{R}$ e $\mathbb{I}$. Ayuda: escriba $\mathbb{I}$ como una unión $\mathbb{I} = A \cup B$ con $A \sim \mathbb{I}$, $B \sim \mathbb{N}$ y $A \cap B = \emptyset$ («unión disyunta»), y compare esa unión con $\mathbb{R} = \mathbb{I} \cup \mathbb{Q}$.

6.3. Demuestre que $\mathbb{R} \sim (0,1) \sim [0,1) \sim (0,1] \sim [0,1]$, donde los diversos intervalos son, respectivamente, el intervalo abierto, semi-cerrado a izquierda, semi-cerrado a derecha, y cerrado, de números reales entre 0 y 1.

6.4. Proponga otras inyecciones explícitas entre $\mathbb{N}$ y $\mathbb{N} \times \mathbb{N}$ diferentes de la inyección canónica $n \mapsto (n, n)$. ¿Cuántas inyecciones existen entre esos dos conjuntos? ¿Cuántas biyecciones existen entre ellos? Defienda sus razonamientos.

6.5. Si A_n $(n \in \mathbb{N})$ es una colección de conjuntos enumerables, muestre que $\bigcup A_n = \{a : \exists n(a \in A_n)\}$ es enumerable (unión enumerable de enumerables es enumerable). Ayuda: aproveche $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$.

6.6. Sea T el conjunto de los números reales que son raíces de ecuaciones de grado 3 con coeficientes enteros. Demuestre que $T \sim \mathbb{N}$. Sea Alg el conjunto de los números reales que son raíces de ecuaciones con coeficientes enteros (números algebraicos). Explique por qué $Alg \sim \mathbb{N}$ (ayuda: considere una unión enumerable de enumerables: ejercicio 6.5).

6.7. Por definición, un número real es *trascendente* si y sólo si no es algebraico. Apoyándose en el ejercicio anterior, muestre que el tamaño de los números trascendentes es igual al tamaño de los números reales. Deduzca que hay *muchísimos más* números trascendentes que algebraicos. De esta manera, una vez más, las apariencias nos engañan: aunque en la práctica matemática las aproximaciones algebraicas parecen cubrir todo nuestro espectro intuitivo, en el *universo de las posibilidades* los objetos trascendentes son mucho más comunes.

6.8. Demuestre que si B es infinito $\mathbb{N} \times B \sim B$. Considere el conjunto $A = \mathbb{N} \times \wp(\mathbb{N} \times \mathbb{N})$. ¿A cuáles de los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$ *no puede* ser similar A? Demuestre su respuesta, utilizando, si lo desea, el teorema de Schröder-Bernstein. Para una respuesta *positiva* acerca de cuál de los conjuntos de números es de hecho similar a A, vea el ejercicio 10.3.

Capítulo 7

Números naturales

Contenido

7.1. Axiomas y principio de inducción 68
7.2. Pruebas por inducción 70
7.3. Buen orden 74
7.4. Ejercicios 76

Hemos presentado, hasta el momento, las disyuntivas y las bases mínimas sobre las que se apoya el conocimiento matemático moderno: (1) tres deslindes fundamentales: positividad/negatividad, finitud/infinitud, conectivos/cuantificadores; (2) ciertas bases relacionales, funcionales y operativas, alrededor de la intuición elemental de los conjuntos. En lo que sigue del curso de FUNDAMENTOS, aplicamos esas ideas a la (re)visión de los conjuntos de números usuales. La colección de conjuntos $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ será presentada *acumulativamente* en los capítulos que siguen, construyendo cada uno de los conjuntos *a partir* del conjunto inmediatamente anterior. El estudiante podrá adquirir así una idea de la *arquitectónica* de las matemáticas.

7.1. Axiomas y principio de inducción

El conjunto de los números naturales es un objeto matemático que responde a tres ideas fundamentales: tener un *comienzo*, gobernar el crecimiento de sus elementos mediante una función *sucesor*, y *no permitir regresos descendentes infinitos*. Esta tercera idea es la característica fundamental del conjunto de

los naturales, y puede expresarse, en forma positiva, mediante el siguiente principio:

Principio de inducción (Ind). Para todo $X \subseteq \mathbb{N}$,

$$0 \in X \ \wedge \forall n(n \in X \to n+1 \in X) \ \to \ X = \mathbb{N}.$$

Revisaremos a lo largo del capítulo la fuerza de este principio, pero debe antes recordarse el buen comportamiento de las funciones de suma y multiplicación en los naturales. La suma $(+)$ y la multiplicación $(\cdot)$ son dos funciones $\mathbb{N}\times\mathbb{N} \xrightarrow{+} \mathbb{N}$, $\mathbb{N}\times\mathbb{N} \xrightarrow{\cdot} \mathbb{N}$ que verifican las siguientes propiedades:

A1. Asociatividad: para todos $a, b, c \in \mathbb{N}$, $a + (b + c) = (a + b) + c$ y $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

A2. Conmutatividad: para todos $a, b \in \mathbb{N}$, $a + b = b + a$ y $a \cdot b = b \cdot a$.

A3. Neutros: existen $0, 1 \in \mathbb{N}$ tales que $0 \neq 1$ y para todo $a \in \mathbb{N}$, $a + 0 = a$ y $a \cdot 1 = a$.

A4. Distributividad: para todos $a, b, c \in \mathbb{N}$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

A5. Cancelatividad: para todos $a, b, c \in \mathbb{N}$, $a + b = a + c$ implica $b = c$, y $a \cdot b = a \cdot c$ implica $b = c$ en el caso $a \neq 0$.

A6. Orden total: si se *define* una relación $\leq$ en $\mathbb{N}$ por la fórmula $a \leq b \leftrightarrow \exists n \in \mathbb{N}(n + a = b)$, la relación obtenida es una relación de orden y verifica, para todos $a, b \in \mathbb{N}$, $a \leq b \vee b \leq a$. 0 resulta ser el *primer* elemento de ese orden.

Estas propiedades podrían *demostrarse*, si las operaciones de suma y multiplicación se construyeran conjuntísticamente (algo que puede realizarse en un curso posterior de TEORÍA DE CONJUNTOS). Sin embargo, aquí adoptamos esas propiedades *axiomáticamente*, es decir, como propiedades indemostradas, pero sobre las que puede basarse cualquier argumento posterior que involucre a las operaciones *descritas* por esos axiomas.

$a + 1$ se llama el **sucesor** de a. Las notaciones usuales corresponden a definir 2 (=1+1) como el sucesor de 1, 3 (=2+1) como el sucesor de 2, 4 (=3+1) como el sucesor de 3, y así sucesivamente. Mediante un uso apropiado de los axiomas muchos hechos sobradamente conocidos pueden entonces *demostrarse*, como por ejemplo 2+3=5. En efecto, $2+3 = (1+1)+(2+1) = ((1+1)+2)+1 = (1+(1+2))+1 = (1+(2+1))+1 = ((1+2)+1)+1 = ((2+1)+1)+1 = (3+1)+1 = 4+1 = 5$: la primera igualdad se debe a las definiciones de 2 y 3, la segunda y la tercera utilizan asociatividad,

la cuarta utiliza la conmutatividad, la quinta utiliza asociatividad, la sexta utiliza conmutatividad, y las tres últimas se deben a las definiciones de 3, 4 y 5. Por supuesto, el interés de este tipo de demostraciones es *nulo en la práctica*, pero, no obstante, *valioso en la teoría*, ya que, con un poco de paciencia, el estudiante puede convencerse de que todas las propiedades usuales de la suma y la multiplicación se *reducen* a los principios (A1)-(A6) *únicamente*. El hecho de que todo un universo infinito de posibilidades se reduzca a un número finito de instancias no es en ningún modo trivial: de allí el interés de las axiomatizaciones.

A partir de los axiomas anteriores, otras *pruebas* de hechos conocidos son por ejemplo (donde ab simplifica la notación $a \cdot b$ y donde $a^2 = aa$):

$$2a = a + a$$

$$(a+b)^2 = a^2 + 2ab + b^2.$$

En efecto, $2a = (1+1)\cdot a = (1\cdot a)+(1\cdot a) = (a\cdot 1)+(a\cdot 1) = a+a$, utilizando, respectivamente, la definición del número 2, el axioma A4, el axioma A2, y el axioma A3. Por otro lado, $(a+b)^2 = (a+b)(a+b) = (a+b)a+(a+b)b = a(a+b)+b(a+b) = aa+ab+ba+bb = a^2+ab+ab+b^2 = a^2+2ab+b^2$, utilizando, respectivamente, A4, A2, A4, A1 (la asociatividad es una forma de eliminar paréntesis), A2, y, finalmente, el resultado anterior ($2x = x+x$).

Los axiomas (en particular, A3, A5, A6) y las definiciones de 2, 3, 4, ..., n, $n+1$, ..., aseguran que el orden $\leq$ en $\mathbb{N}$ verifica

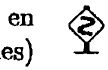
$$0 \leq 1 \leq 2 \leq 3 \leq \cdots \leq n \leq n+1 \cdots$$

donde $n \neq n+1$ y entre n y $n+1$ no existe ningún otro natural distinto de ellos. Se trata de un orden muy peculiar, en el cual, como se puede *intuir* en el dibujo, *no existen cadenas descendentes infinitas* (por supuesto, sí existen cadenas ascendentes infinitas). La *fundamentación* de esa intuición se encuentra en el principio de inducción, que pasamos a revisar a continuación.

7.2. Pruebas por inducción

Las pruebas por inducción constituyen la operatoria demostrativa fundamental en el ámbito de los números naturales. Las pruebas por inducción se refieren a *propiedades* cuyo espectro de validez debe *cubrir todo* $\mathbb{N}$. Informalmente, en el universo de los naturales sucede *siempre* que si una propiedad

vale en un *comienzo*, y vale la *transmisión* de la verdad de $P(n)$ a la verdad de $P(n+1)$, entonces la propiedad vale *para todos* los naturales por encima de ese comienzo. El interés de este tipo de argumentos consiste, de nuevo, en *reducir* una frase complicada de verificar (un hecho *para todos* los naturales) a un par de verificaciones más sencillas (comienzo, transmisión al sucesor). Formalmente, una prueba por inducción sigue entonces el esquema:



Prueba por inducción (PI). Para toda $P(a)$ propiedad que se refiera a números naturales,

$$P(0) \ \wedge \forall n \in \mathbb{N}(P(n) \rightarrow P(n+1)) \ \rightarrow \ \forall n \in \mathbb{N}\, P(n).$$

Las pruebas por inducción corresponden a un manejo *intensional* (ver sección 2.1) de las bases *extensionales* codificadas en el principio de inducción (**Ind**). De manera más precisa, se tiene la equivalencia

Ind si y sólo si **PI**.

En efecto, asuma **Ind** y sea $P(a)$ una propiedad que se refiera a los naturales, tal que vale $P(0)$ y vale el paso $P(n) \rightarrow P(n+1)$. Considere entonces $X = \{n \in \mathbb{N} : P(n)\}$. Por las hipótesis en juego, tenemos que $0 \in X$ (pues vale $P(0)$) y que $n \in X \rightarrow n+1 \in X$ (pues vale $P(n) \rightarrow P(n+1)$). Por el principio de inducción (**Ind**) aplicado a X, se tiene entonces que $X = \mathbb{N}$, pero esto quiere decir que $P(n)$ vale para todo natural. Hemos demostrado así (**PI**). Viceversa, asuma (**PI**) y sea X un subconjunto de naturales que contenga al 0 y para el cual valga el paso $n \in X \rightarrow n+1 \in X$. Considere entonces la propiedad P «ser elemento de X»: $P(n) \leftrightarrow n \in X$. Por las hipótesis, vale $P(0)$ (pues $0 \in X$) y vale el paso $P(n) \rightarrow P(n+1)$ (pues $n \in X \rightarrow n+1 \in X$). Gracias al esquema de pruebas por inducción (**PI**) aplicado a P, se tiene entonces que $P(n)$ vale para todos los naturales, pero esto quiere decir que $X = \mathbb{N}$. Hemos probado así (**Ind**).

Una vez asumido el principio de inducción (**Ind**), hemos *demostrado* que podemos entonces contar con pruebas por inducción en los naturales. Se trata de un procedimiento *ubicuo* de prueba, que el estudiante encontrará incesantemente en los más diversos ámbitos de la Carrera de Matemáticas.

Las pruebas por inducción pueden restringirse a ciertos subconjuntos de los naturales. Si se logra demostrar, por ejemplo, que vale $P(a_0)$ para algún a_0 natural, y que vale la transmisión $P(n) \rightarrow P(n+1)$ *a partir* de a_0, entonces la propiedad $P(a)$ valdrá para todo $a \geq a_0$ (ver ejercicio 7.4). Se tiene así el siguiente esquema de prueba por inducción truncada:

Prueba por inducción truncada ($\mathbf{PI}_{\geq}$). Para toda $P(a)$ propiedad que se refiera a números naturales, para todo $a_0 \in \mathbb{N}$,

$$P(a_0) \wedge \forall n \geq a_0 (P(n) \to P(n+1)) \quad \to \quad \forall n \geq a_0 \; P(n).$$

Ejemplo 7.1. Las siguientes propiedades son válidas para *todos* los naturales $n \geq 1$ y pueden demostrarse por inducción (truncada, empezando desde 1, aunque en algunos casos también vale desde 0):

(i) $1+2+3+\cdots+n = \frac{n(n+1)}{2}$

(ii) $1+3+5+\cdots+(2n-1) = n^2$

(iii) $1^3+2^3+3^3+\cdots+n^3 = (\frac{n(n+1)}{2})^2$

(iv) $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)} = \frac{n}{n+1}$

(v) $6 \mid n(n+1)(n+2)$

(vi) $13 \mid 4^{2n+1}+3^{n+2}$

(vii) $3 \mid n^4-4n^2$

(viii) $\overline{\overline{\wp(\{1,2,\ldots,n\})}} = 2^n$

(ix) El número de inyecciones de $\{1,2,\ldots,n\}$ en $\{1,2,\ldots,m\}$ es igual a $m(m-1)\cdots(m+1-n)$ si $n \leq m$.

Observemos algunas de estas pruebas (las demás se remiten al ejercicio 7.6). Para el caso (i), sea $P(n)$ la propiedad «$1+2+3\cdots+n = \frac{n(n+1)}{2}$». $P(1)$ vale trivialmente pues $1 = \frac{1(1+1)}{2}$. Por otro lado, si $P(n)$ vale entonces $1+2+3\cdots+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$, es decir que $P(n+1)$ vale. Por inducción, se tiene entonces $P(n)$ para todo $n \geq 1$.

Para el caso (iv), sea $P(n)$ la propiedad «$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)} = \frac{n}{n+1}$». $P(1)$ vale trivialmente pues $\frac{1}{1\cdot 2} = \frac{1}{1+1}$. Por otro lado, si $P(n)$ vale entonces $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}+\frac{1}{(n+1)(n+2)} = \frac{n}{n+1}+\frac{1}{(n+1)(n+2)} = \frac{n(n+2)+1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2}$, es decir que $P(n+1)$ vale. Por inducción, se tiene entonces $P(n)$ para todo $n \geq 1$.

Para el caso (vii), sea $P(n)$ la propiedad «$3 \mid n^4-4n^2$». $P(1)$ vale trivialmente pues $3 \mid -3 = 1^4-4(1^2)$ (observe que puede empezar aquí también desde 0, pues $P(0)$ también vale). Por otro lado, si $P(n)$ vale, se tiene que $3 \mid n^2(n^2-4) = n^2(n-2)(n+2)$; como 3 es primo, esto significa que 3 divide

a alguno de esos tres factores: n, $n-2$ o $n+2$. Se tiene $(n+1)^4-4(n+1)^2 = (n+1)^2((n+1)^2-4) = (n+1)^2(n^2+2n-3) = (n+1)^2(n-1)(n+3)$. Ahora bien, si $3 \mid n$ entonces $3 \mid (n+3)$; si $3 \mid (n-2)$ entonces $3 \mid (n+1)$; y si $3 \mid (n+2)$ entonces $3 \mid (n-1)$. En todos los casos, $3 \mid (n+1)^4-4(n+1)^2$, es decir $P(n+1)$ vale. Por inducción, se tiene entonces $P(n)$ para todo $n \geq 1$. Obsérvese que, en este caso, la prueba por inducción *no es más cómoda* que una prueba directa del mismo hecho (obtenida en la mitad de este párrafo, pues 3 *siempre* divide a alguno de los tres factores n, $n-2$ o $n+2$: compruébelol).

Para el caso (ix), sea m un natural fijo. Sea $P(n)$ la propiedad «el número de inyecciones de $\{1,2,\ldots,n\}$ en $\{1,2,\ldots,m\}$ es igual a $\varphi(n) = m(m-1)\cdots(m+1-n)$ si $n \leq m$». $P(1)$ vale pues el número de inyecciones de un conjunto de 1 elemento en un conjunto de m elementos es obviamente m (igual al número de funciones en este caso), y también $m = \varphi(1)$. Suponga ahora que $P(n)$ vale, y sea $n+1 \leq m$. El número de inyecciones del conjunto $\{1,2,\ldots,n+1\}$ en $\{1,2,\ldots,m\}$ se calcula obteniendo el número de inyecciones de $\{1,2,\ldots,n\}$ en $\{1,2,\ldots,m\}$ (que dejan a $n+1$ libre), y combinándolo con el número de posibles imágenes de $n+1$ que *no repitan* elementos en el codominio (para poder preservar así la inyectividad). El primero de los números en la frase anterior es $\varphi(n)$ (por hipótesis de inducción), y el segundo es $m-n$, el número de «casillas» que no fueron usadas en el codominio de las inyecciones. El número de inyecciones del conjunto $\{1,2,\ldots,n+1\}$ en $\{1,2,\ldots,m\}$ es entonces $\varphi(n)\cdot(m-n) = \varphi(n+1)$. Lo anterior demuestra el paso de transición y, por inducción, se tiene entonces $P(n)$ para todo $n \geq 1$. Puede observarse aquí también que una prueba *directa* del resultado (por descarte sucesivo de posibilidades para las imágenes en una inyección) es más fácil que la prueba por inducción recién señalada. La prueba por inducción proporciona, no obstante, una calidad de *rigor* que no se consigue con la prueba visual directa.

En algunos casos, para realizar una prueba de inducción más cómoda, resulta útil intentar el paso de transición hacia $P(n+1)$, no sólo con la información disponible en $P(n)$, sino con *toda la información previa*: $P(0)$, $P(1)$, ..., $P(n)$. Tenemos entonces lo que se llama una prueba por inducción completa:

Prueba por inducción completa (PIC). Para toda $P(a)$ propiedad que se refiera a números naturales,

$$P(0) \wedge \forall n \in \mathbb{N}(\forall i(i \leq n \rightarrow P(i)) \rightarrow P(n+1)) \quad \rightarrow \quad \forall n \in \mathbb{N}\ P(n).$$

En el caso de tener que realizar una inducción completa truncada, basta con tener en cuenta la información acumulada desde $P(a_0)$.

Ejemplo 7.2. Podemos ahora sí *demostrar* el teorema fundamental de factorización en primos (usado, por ejemplo, en el ejercicio 1.5): para todo n natural, $n \geq 2$, existen primos p_i y exponentes $\alpha_i \geq 1$ tales que $n = \prod p_i^{\alpha_i}$. El teorema es claro para $n = 2$ (desde donde comienza la inducción truncada), pues 2=2: se factoriza a sí mismo como primo. Suponiendo ahora el resultado para todo i, $2 \leq i \leq n$, considérese a $n+1$. Si $n+1$ es primo, él se factoriza a sí mismo. Si no es primo, $n+1 = ab$, con $a, b < n+1$, es decir $a, b \leq n$. Por hipótesis de inducción (completa), a y b se factorizan como productos de primos, y entonces también $ab = n+1$ es un producto de primos.

Ejemplo 7.3. Demuestre que $\forall n \geq 10(2^n > n^3)$. Haciendo los cálculos, observe primero que el resultado no es cierto si $n \leq 9$; la prueba por inducción (truncada) debe entonces empezar en $n = 10$, pues para 10 sí se tiene $2^{10} = 1024 > 1000 = 10^3$. Por otro lado, asuma, por inducción completa, que $(2^i > i^3)$, para $10 \leq i \leq n$. Entonces, $2^{n+1} = 2^n + 2^n > 2^n + 2^{n-1} > n^3 + (n-1)^3 > (n+1)^3$. La segunda desigualdad usa la inducción completa (en realidad sólo los dos casos para n y $n-1$), y la tercera desigualdad corresponde (después de desarrollar las potencias y simplificar) a $n^3 > 6n^2 + 2$, algo que es inmediato de chequear para $n \geq 7$ (y con mayor razón para $n \geq 10$).

7.3. Buen orden

Explicamos ahora brevemente cómo el principio de inducción en los naturales evita la posibilidad de que existan cadenas infinitas descendentes en $\mathbb{N}$.

Definición 7.4. Sea $(A, \leq)$ un conjunto ordenado (es decir, un conjunto con una relación de orden $\leq$ en A). $(A, \leq)$ está **bien ordenado** si y sólo si todo subconjunto X no vacío de A posee un mínimo elemento (dentro del *mismo* X, por definición de mínimo):

$$\forall X \subseteq A(X \neq \emptyset \rightarrow \exists m \in A \; m = min(X))$$

donde $m = min(X)$ codifica la frase $(m \in X \wedge \forall a \in X m \leq a)$.

De la definición misma, se sigue que un conjunto bien ordenado no posee cadenas infinitas descendentes, pues toda cadena debe tener un mínimo. Esto

es algo que *no* sucede con los otros conjuntos usuales de números ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) donde sí existen cadenas infinitas descendentes. De hecho, una manera de expresar la *especificidad* del conjunto $\mathbb{N}$ entre los demás conjuntos usuales de números consiste en afirmar que $(\mathbb{N}, \leq)$ (orden usual) está *bien ordenado*. En efecto, tenemos la proposición:

Teorema 7.5. ***Ind*** *si y sólo si* $(\mathbb{N}, \leq)$ *está bien ordenado.*

Demostración. Obsérvese primero que, cuando $X \subseteq \mathbb{N}$, el principio de inducción (**Ind**) aplicado al complemento X^c asegura que si tenemos $0 \in X^c$ y $\forall n(n \in X^c \to n+1 \in X^c)$ entonces $X^c = \mathbb{N}$, es decir, $0 \notin X$ y $\forall n(n \notin X \to n+1 \notin X)$ implica $X = \emptyset$. Para mostrar que un subconjunto X de naturales es vacío basta así con demostrar que 0 no pertenece a X y que si n no pertenece a X, $n+1$ tampoco debe pertenecer a X.

Suponga ahora el principio de inducción (**Ind**), vamos a *indicar* cómo los naturales están bien ordenados (una prueba totalmente rigurosa requiere utilizar inducción completa y el ejercicio 7.5, pero es asequible para un buen estudiante: realícela!). Sea X un subconjunto no vacío de naturales. Si $0 \in X$, automáticamente $0 = min(X)$ y el mínimo pertenece a X. Podemos suponer entonces $0 \notin X$. Por el comentario del párrafo anterior, no podemos tener, para todo n, $(n \notin X \to n+1 \notin X)$, pues si no $X = \emptyset$, contradiciendo el hecho de que hemos tomado X no vacío. *Existe* entonces $n \notin X$, $n+1 \in X$. Enumérense todos los elementos por debajo de n: como sólo hay un *número finito* de ellos, será posible detectar cuáles elementos no pertenecen a X, y el primero que pertenezca a X será el mínimo de X. Este argumento, que depende de (**Ind**), *reduce un posible problema de infinitud a un conteo finito*: en efecto, X puede ser infinito y, en los casos interesantes, siempre lo es.

Viceversa, si suponemos buen orden en los naturales, el principio de inducción se demuestra sin más requerimientos. Sea X un subconjunto de naturales tal que $0 \in X$ y $\forall n(n \in X \to n+1 \in X)$ (*). Considere $Y = X^c$. Mostramos, por contradicción, que $Y = \emptyset$, por lo tanto $X = \mathbb{N}$, como se desea en el principio de inducción. Suponga entonces $Y \neq \emptyset$; por el buen orden, Y tendría un mínimo $m \in Y = X^c$. Tenemos $m \neq 0$ puesto que $0 \in X$. Podemos considerar entonces el antecesor $m-1$ (existe pues m no es 0); como m era el mínimo en $Y = X^c$, se sigue que $m-1 \notin Y$, es decir $m-1 \in X$; pero X verificaba la propiedad de transición (*): entonces $m \in X$, y se tiene la contradicción $m \in X \cap X^c = \emptyset$.

□

7.4. Ejercicios

7.1.Partiendo *únicamente* de la definición ($a \leq b \leftrightarrow \exists n \in \mathbb{N}(n + a = b)$), de los axiomas (A1)-(A5) y de $1 \not\leq 0$, demuestre que $\leq$ es una relación de orden en $\mathbb{N}$ (reflexiva, antisimétrica, transitiva), con mínimo elemento 0, no simétrica, tal que $0 \leq 1 \leq 2 \leq 3 \leq \cdots \leq n \leq n+1 \cdots$, y tal que no existe ningún natural entre n y $n+1$ distinto de ellos.

7.2. Demuestre, siguiendo cuidadosamente los axiomas y la definición del número 3, que $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$, para todos $a, b \in \mathbb{N}$ (donde $a^3 = a^2a$ por definición).

7.3. Demuestre, siguiendo cuidadosamente los axiomas, que $a0 = 0$ para todo $a \in \mathbb{N}$.

7.4. Demuestre que **(PI)** y **(PI$_\geq$)** son equivalentes.

7.5. Demuestre que **(PI)** y **(PIC)** son equivalentes.

7.6. Demuestre las aserciones del ejemplo 7.1 que no fueron probadas en el cuerpo del texto.

7.7. Demuestre por inducción las siguientes proposiciones. Haga explícita cuál forma de inducción utiliza (sencilla, truncada o completa) y precise desde *cuál* natural vale la inducción.

(i) $T_1 + T_2 + \cdots + T_n = \frac{n(n+1)(n+2)}{6}$, donde T_n es el n-ésimo número triangular (de esta manera la fórmula que usted debió *encontrar* en el ejercicio 1.3, es ahora capaz de *demostrarla*: ha logrado pasar del ámbito de lo *empírico* al ámbito de lo *necesario*!)

(ii) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

(iii) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$

(iv) si $r \in \mathbb{R}$, $r \neq 1$, $1 + r + r^2 + \cdots + r^n = \frac{1-r^{n+1}}{1-r}$

(v) $8 \mid 13^n - 5^n$

(vi) $3 \mid 2^{2n} - 1$ y $8 \mid 3^{2n} - 1$

(vii) $n^2 < 2^n$

(viii) $n! < \frac{(n+1)^n}{2}$.

7.8. Se define una colección de números reales mediante las reglas $a_0 = 1$, $a_{n+1} = \sqrt{(1 + a_n)}$. Muestre, por inducción sobre n, que para todo $n \in \mathbb{N}$ se tiene $a_n < 2$.

7.9. Sean a_i, b_i $(1 \leq i \leq n)$ números reales tales que $a_1 \geq a_2 \geq \cdots \geq a_n$ y $b_1 \geq b_2 \geq \cdots \geq b_n$. Demuestre, por inducción sobre n, que vale $(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n) \leq n(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n)$ (desigualdad de Chebichev). Ayuda: para el paso por inducción, demuestre antes la propiedad del «intercambio» $xy + zt \leq xz + yt$ cuando $y \geq z$ y $t \geq x$ $(x, y, z, t \in \mathbb{R})$ (prueba fácil); luego, en el curso de la inducción, ordene adecuadamente los términos para poder usar un «intercambio» propicio (prueba más delicada).

7.10. Considere la siguiente «prueba» por inducción.

Proposición. Todos los conjuntos finitos de mismo cardinal son iguales. Prueba por inducción simple sobre $n \geq 0$ (n es el cardinal del conjunto). Paso inicial: dos conjuntos cualesquiera sin elementos son iguales. Paso de inducción: suponga que todos los conjuntos con n elementos son iguales. Sean A y B dos conjuntos con $n + 1$ elementos. Por hipótesis de inducción, los n primeros elementos de A son iguales a los n primeros elementos de B. De la misma manera, los n últimos elementos de A son iguales a los n últimos elementos de B. Por lo tanto, A y B poseen los mismos elementos, y se tiene $A = B$.

Aunque la proposición anterior es evidentemente falsa (el conjunto $\{1, 2\}$ no es igual al conjunto $\{2, 3\}$) la prueba anterior parece completamente correcta. ¿Dónde está el error?

Capítulo 8

Números enteros y racionales

Contenido

8.1. Construcción de los números enteros 79
8.2. Más sobre divisibilidad en $\mathbb{Z}$ 86
8.3. Números racionales 89
8.4. Ejercicios 92

El capítulo anterior ha presentado algunas de las propiedades del conjunto de los números naturales, que debe entenderse como el *primer* conjunto infinito (un *axioma* posterior en TEORÍA DE CONJUNTOS postulará que $\mathbb{N}$ es en realidad una forma inicial de infinitud). *A partir* de $\mathbb{N}$ surgen los demás conjuntos usuales de números, por medio de procesos de «saturación» con respecto a las *diversas propiedades* potenciales de las operaciones y las relaciones inherentes en $\mathbb{N}$. Un primer paso consiste en «completar» las operaciones de *suma* y *multiplicación*: proveer inversos para la suma y proveer inversos para la multiplicación. En este primer paso, se obtienen los enteros ($\mathbb{Z}$) y los racionales ($\mathbb{Q}$), de los cuales nos ocupamos en este capítulo. Un segundo paso consistirá en «completar» ciertas operaciones de *aproximabilidad* en el infinito (proveer límites para sucesiones); de allí surgirán los números reales ($\mathbb{R}$). Un tercer paso consistirá en «completar» las *soluciones polinomiales* (proveer números extendidos para resolver ecuaciones); de allí surgirán los números complejos ($\mathbb{C}$). En el curso de FUNDAMENTOS alcanzaremos a cubrir estos tres pasos, pero éstos no son más que el inicio de una larga serie de *aperturas hacia mundos posibles* que irán respondiendo a diversas problemáticas a lo largo de toda la Carrera de Matemáticas.

8.1. Construcción de los números enteros

La idea básica en la construcción de los números enteros consiste en definir un universo de números en el cual puedan ser resueltas *todas* las ecuaciones lineales del tipo $x + y = z$. Esto se realiza gracias a la resta $y = z - x$, pero ésta no siempre existe en $\mathbb{N}$, pues la definición misma del orden en $\mathbb{N}$ (ver axioma 6 del capítulo anterior) exige que para resolver $x + y = z$ en $\mathbb{N}$ se debe tener $x \leq z$. Ahora bien, un número puede escribirse como una resta de *múltiples* maneras (manejamos por ahora ideas intuitivas, pronto daremos las definiciones más rigurosas del caso):

$$7 = 7 - 0 = 8 - 1 = 9 - 2 = \cdots = (n + 7) - n = \cdots$$

$$-2 = 0 - 2 = 1 - 3 = 2 - 4 = \cdots = n - (n + 2) = \cdots$$

Obsérvese entonces que los enteros positivos pueden *representarse* gracias a parejas de naturales (x, y) donde $x \geq y$, y los enteros negativos gracias a parejas de naturales (x, y) con $x \leq y$. Dentro de las múltiples (de hecho, *infinitas*) parejas de naturales que pueden representar un número, habría que poder *identificar* ciertas buenas expresiones en detrimento de otras (por ejemplo, -2 «bien» representado por $(2, 4)$, «mal» representado por $(7, 10)$). De lo anterior, se infiere que una construcción *no artificial* de los enteros debe poder manejar: (i) parejas de naturales; (ii) procesos de identificación entre entes matemáticos.

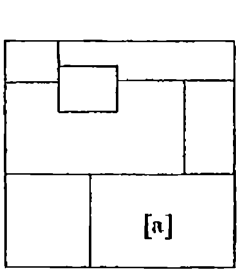
El instrumentario canónico en matemáticas para identificar objetos es el de las relaciones de equivalencia (ver comentario después del ejemplo 4.5). Una relación de equivalencia (reflexiva, simétrica y transitiva) *generaliza* de hecho las propiedades de la igualdad, con la que se identifican de la manera más fuerte posible un par de objetos: la igualdad es trivialmente reflexiva $(x = x)$, simétrica $(x = y \to y = x)$ y transitiva $(x = y \wedge y = z \to x = z)$. Las relaciones de equivalencia permiten entonces «identificar» ciertos objetos matemáticos de una manera más *suave*, sin que sean trivialmente iguales, pero sí lo suficientemente parecidos con respecto a ciertas propiedades dadas.

Definición 8.1. Sea R una relación de equivalencia sobre un conjunto A no vacío. Si $a \in A$, la **clase de equivalencia de a (módulo R)** (notación $[a]_R$) se define como el subconjunto de elementos de A relacionados con a bajo R: $[a]_R = \{x \in A : xRa\}$.

Las propiedades *conjuntistas* de las clases de equivalencia son muy peculiares. Son no vacías: para todo $a \in A$, $a \in [a]_R$ gracias a que la relación es

reflexiva. Son «recubridoras»: todo elemento de A está en al menos una clase de equivalencia, a saber en la clase de él mismo (de nuevo, porque $a \in [a]_R$). Son disyuntas dos a dos, es decir, si $[a]_R \neq [b]_R$ entonces $[a]_R \cap [b]_R = \emptyset$. En efecto, suponga $[a]_R \neq [b]_R$; esto es *equivalente* a decir no aRb (chequéelo!). *Por contradicción*, suponga ahora que $[a]_R \cap [b]_R \neq \emptyset$: existe $c \in [a]_R \cap [b]_R$ y tenemos cRa y cRb. Como R es simétrica, de cRa se deduce aRc, y como R es transitiva, de aRc y cRb se deduce aRb, lo que genera una contradicción (con no aRb). Observe cómo en la prueba se han usado las tres propiedades fundamentales: reflexividad, simetría, transitividad.

Las clases de equivalencia de R constituyen así una suerte de *compartimentación* del conjunto subyacente A. Esta situación se llama una *partición* de A, como lo señalamos a continuación.



Definición 8.2. Sea A un conjunto no vacío. Una **partición** de A consiste en darse una colección no vacía $\mathcal{C}$ de subconjuntos de A (llamados «celdas») con las propiedades siguientes:

(*i*) $X \in \mathcal{C} \rightarrow X \neq \emptyset$

(*ii*) $X, Y \in \mathcal{C} \wedge X \neq Y \rightarrow X \cap Y = \emptyset$

(*iii*) $\bigcup_{X \in \mathcal{C}} X = A$

(donde esta tercera propiedad expresa que la unión de todos los subconjuntos $X \in \mathcal{C}$ es igual a todo A, o, dicho de otra manera, que todo elemento de A pertenece al menos a algún subconjunto $X \in \mathcal{C}$).

Un hecho fundamental consiste en que, sobre un conjunto no vacío dado, las relaciones de equivalencia se *corresponden perfectamente* con las particiones. Dada una relación de equivalencia, las clases de equivalencia de la relación constituyen una partición (es lo que mostramos justamente después de la definición 8.1). Y viceversa, dada una partición, la relación que consiste en pertenecer a una misma celda es una relación de equivalencia (demuestre todo esto en el ejercicio 8.1).

Una vez establecido este *instrumentario fundacional* alrededor de las relaciones de equivalencia, clases de equivalencia y particiones, podemos volver ahora al *caso particular* de las identificaciones entre parejas de naturales con las que abrimos esta sección.

Deseamos *construir* los enteros como *clases de parejas de naturales*, siguiendo las constataciones expresadas en las identidades

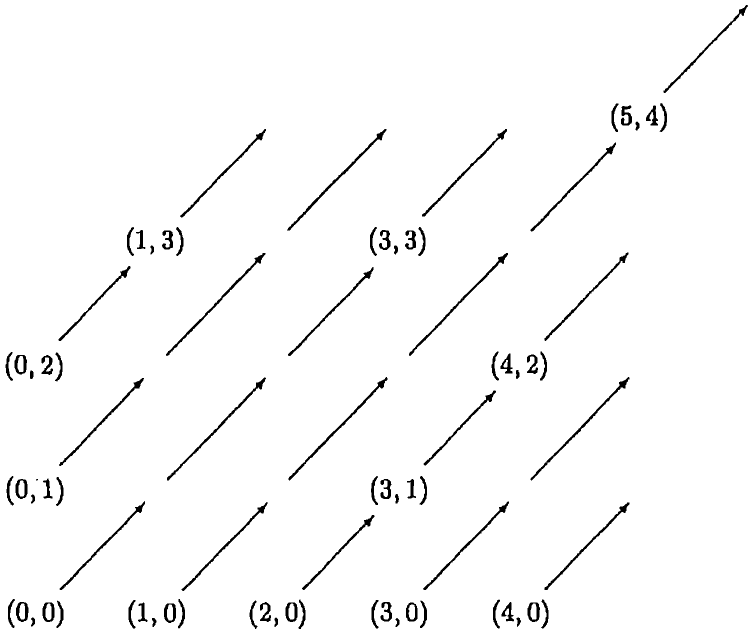
$$7 = 7 - 0 = 8 - 1 = 9 - 2 = \cdots = (n + 7) - n = \cdots$$

$$-2 = 0 - 2 = 1 - 3 = 2 - 4 = \cdots = n - (n + 2) = \cdots$$

Observe que, para cualquiera de los dos casos, *independientemente de la positividad o negatividad del número*, las parejas (a, b) o (c, d) que pretendan poder representar al número verifican siempre $a - b = c - d$, *es decir* $a + d = b + c$ (*). El punto fundamental en esta segunda ecuación es que *no mencionamos* la resta y *no mencionamos* números negativos, sino sólo naturales. Esto indica que mediante la suma, mediante parejas de naturales y mediante la relación (*), podrá reconstruirse la idea de resta. Este es el camino que adoptamos ahora, dejando de lado las intuiciones originarias, para *definir formalmente* al conjunto $\mathbb{Z}$.

Ejemplo 8.3. Sea R la relación en $\mathbb{N} \times \mathbb{N}$ definida por $(a, b)R(c, d)$ si y sólo si $a + d = b + c$ (informalmente, «primero más cuarto es igual a segundo más tercero»). Se trata de una relación entre parejas de naturales: si desea ser riguroso, compruebe que $R \subseteq \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$. Tenemos que R es una *relación de equivalencia*. En efecto, es reflexiva pues $(a, b)R(a, b)$ ya que $a + b = b + a$ (gracias al axioma de *conmutatividad* de la suma). Es simétrica pues $(a, b)R(c, d)$ significa $a + d = b + c$, lo que implica $c + b = d + a$ (por la conmutatividad de nuevo), y esto significa $(c, d)R(a, b)$ («primero más cuarto es segundo más tercero»). Es transitiva pues $(a, b)R(c, d)$ y $(c, d)R(e, f)$ significa $a + d = b + c$ y $c + f = d + e$, lo que implica $a + d + f = b + c + f = b + d + e$ (gracias al axioma de *asociatividad* de la suma), lo que implica $a + f + d = b + e + d$ (por conmutatitividad), lo que implica $a + f = b + e$ (cancelando d, gracias al axioma de *cancelatividad* de la suma), pero esto significa $(a, b)R(e, f)$ («primero más cuarto es segundo más tercero»).

Esta relación particiona entonces $\mathbb{N} \times \mathbb{N}$ en clases de equivalencia, como se puede observar en el diagrama siguiente. En el diagrama las diagonales marcadas son las *clases de equivalencia* de la relación R recién estudiada en el ejemplo. Puede observarse que hay infinitas clases de equivalencia (infinitas diagonales), y que cada clase de equivalencia es a su vez infinita (infinitos puntos en cada diagonal).



Las diagonales son las clases de equivalencia; por ejemplo, $[(2,0)]_R = \{(2,0),(3,1),(4,2),\ldots,(n+2,n),\ldots\}$. Las diagonales que parten de las parejas del tipo $(n,0)$ representarán a los números *enteros positivos*. Las diagonales que parten de las parejas del tipo $(0,n)$ representarán a los números *enteros negativos*. Podemos ya definir formalmente al conjunto de los enteros.

Definición 8.4. Sea R la relación de equivalencia entre parejas de naturales definida en el ejemplo 8.3. El conjunto de los números enteros $\mathbb{Z}$ se define por:

$$\mathbb{Z} = \{[(a,b)]_R : (a,b) \in \mathbb{N} \times \mathbb{N}\}.$$

Las operaciones de suma y multiplicación en $\mathbb{Z}$ se definen por:

$$[(a,b)]_R + [(c,d)]_R = [(a+c, b+d)]_R$$

$$[(a,b)]_R \cdot [(c,d)]_R = [(ac+bd, ad+bc)]_R.$$

Obsérvese que las operaciones de suma y multiplicación son ahora *entre clases de equivalencia*. Son operaciones que *no* son inmediatamente evidentes: en esta primera instancia, estamos sumando y multiplicando «diagonales»! No obstante, pronto reemplazaremos las clases por símbolos más sencillos que las denoten, y llegaremos a los cálculos intuitivamente conocidos en $\mathbb{Z}$.

Un primer punto fundamental con la nueva suma es que *hemos obtenido inversos*! Es claro ante todo que la clase $[(0,0)]_R$ actúa como neutro para la suma: $[(a,b)]_R + [(0,0)]_R = [(a+0, b+0)]_R = [(a,b)]_R$. Ahora, *para todo* $[(a,b)]_R$, podemos encontrar $[(c,d)]_R$ que sirva de inverso, es decir tal que $[(a,b)]_R + [(c,d)]_R = [(0,0)]_R$. En efecto, la ecuación anterior *nos fuerza* a que $[(a+c, b+d)]_R = [(0,0)]_R$, lo que significa $a+c+0 = b+d+0$, es decir $a+c = b+d$: tomando $c = b$ y $d = a$ la ecuación se satisface (gracias a la conmutatitivad de la suma en $\mathbb{N}$: siempre aparece escondida). Esto muestra que la clase $[(b,a)]_R$ sirve entonces justamente como *inverso aditivo* de la clase $[(a,b)]_R$.

Debe tenerse algo de cuidado con las definiciones de suma y multiplicación en $\mathbb{Z}$ que hemos introducido en la definición 8.4, pues estamos definiendo las operaciones entre clases de equivalencia por medio de algunos *elementos* en las clases («representantes» de las clases). Como las clases son grandes (y, en este caso particular, infinitas!), si cambiáramos los elementos de las clases podría, en principio, cambiar el resultado de las operaciones. En realidad, eso no sucede, pues la relación R se «comporta bien» con respecto a la suma y multiplicación de naturales (véase el ejercicio 8.2). Este es un caso particular de «buenos comportamientos» de ciertas relaciones de equivalencia con respecto a ciertas operaciones. Esas «buenas» relaciones de equivalencia se llamarán *congruencias*, y, en buena medida, los comienzos de cursos posteriores en ÁLGEBRA ABSTRACTA, TEORÍA DE CUERPOS, ÁLGEBRA CONMUTATIVA o ÁLGEBRA UNIVERSAL entrarán a estudiar con todo detenimiento esas congruencias en ámbitos muy generales.

Para simplificar la presentación de los objetos con los cuales estamos trabajando, introducimos las **notaciones estándar** asociadas a estas clases de equivalencia. Por medio de la inyección $\mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N} : n \mapsto [(n,0)]_R$ (chequear que es 1-1!) podemos identificar n con su clase de equivalencia asociada $[(n,0)]_R$. Por otro lado, *definimos*

$$-n = [(0,n)]_R.$$

Aparecen así finalmente los **números negativos**, construidos únicamente *desde* los naturales. Con estas notaciones se tiene la ley fundamental de los enteros, la ley que le otorga una *especificidad* propia a $\mathbb{Z}$:

$$-n+n=[(0,n)]_R+[(n,0)]_R=[(n,n)]_R=[(0,0)]_R=0.$$

La primera igualdad se debe a las notaciones para $-n$ y n, la segunda a la suma en $\mathbb{Z}$, la tercera al hecho de que $(0,0)$ y (n,n) están relacionados bajo R (por tanto están en la misma clase de equivalencia, y sus clases de equivalencia son iguales), la cuarta a la notación para 0.

Puede chequearse (aunque aquí, en cambio, *no* aconsejamos que lo haga el estudiante: poco ganará con ello) que las operaciones de suma y multiplicación definidas en $\mathbb{Z}$ *continúan verificando* las propiedades (A1)-(A5) que se tenían para las operaciones de suma y multiplicación entre naturales. También, el orden total (A6) sigue valiendo entre enteros mediante la fórmula $n \leq m \leftrightarrow \exists s \in \mathbb{N}(n+s=m)$, pero aquí es fundamental mantener la existencia de s en $\mathbb{N}$. La gran ganancia obtenida consiste en una «ampliación» o «compleción» de la parte aditiva del axioma (A3). Se han obtenido en efecto inversos para la suma:

$$\forall a \in \mathbb{Z}\ \exists b \in \mathbb{Z}\ a+b=0.$$

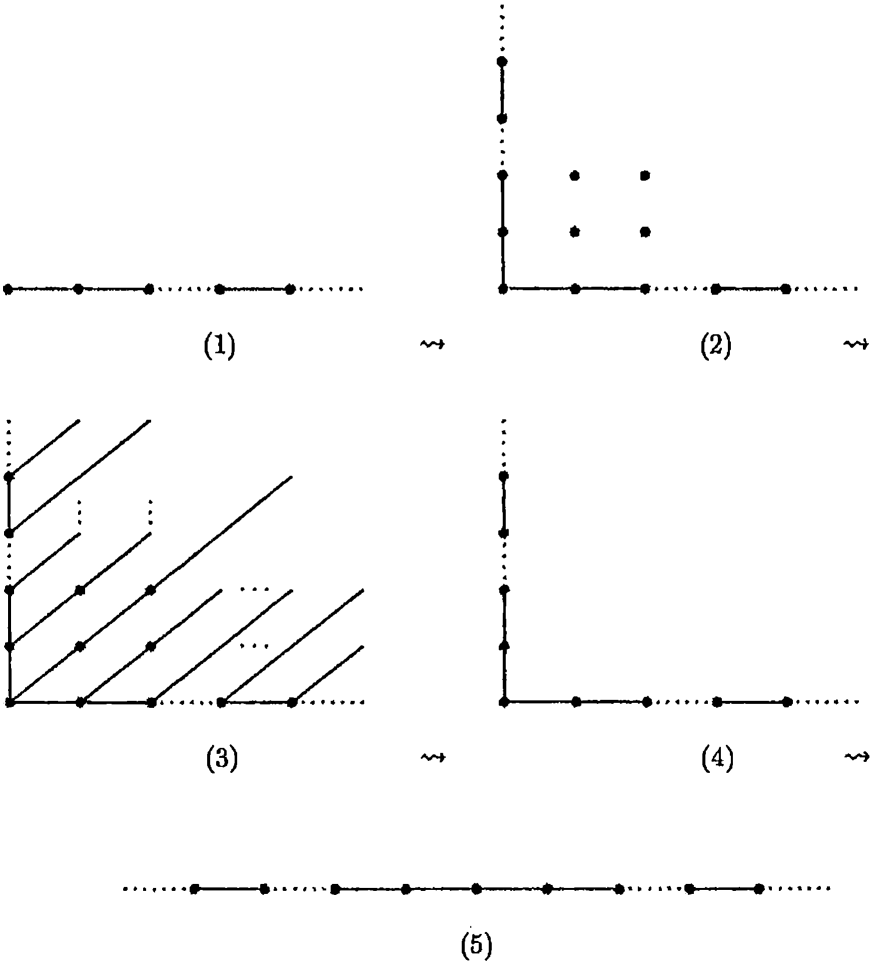
Ahora bien, lo que por un lado se gana, por otro lado se pierde. En el conjunto de los enteros *falla el principio de inducción*. De hecho, en $\mathbb{Z}$ hay cadenas descendentes infinitas,

$$\cdots \leq -n-1 \leq -n \leq \cdots \leq -3 \leq -2 \leq -1 \leq 0$$

y, como hemos visto en la sección 7.3, esto es algo que va en contravía del principio de inducción. Entiéndase bien entonces lo que se ha logrado: (i) *construir* un conjunto partiendo *desde* otro, y empezar así a *elevar un edificio*; (ii) responder con ello a la problemática de la resolución de *todas* las ecuaciones lineales sin coeficientes $x+y=z$. Si el ámbito propio para argumentos de inducción es el ámbito de los naturales, el ámbito propio para argumentos ligados a ecuaciones un poco más delicadas es el ámbito de los enteros, como quedará patente en la sección 8.2.

Desde un punto de vista meramente *geométrico*, es útil subrayar cómo se ha realizado la construcción de $\mathbb{Z}$, a partir de $\mathbb{N}$. En las gráficas de la página siguiente se parte (1) de la semi-recta discreta $\mathbb{N}$, se pasa (2) al cuadrante superior derecho discreto $\mathbb{N}\times\mathbb{N}$, se trazan (3) todas las diagonales paralelas

a la diagonal principal (clases de equivalencia módulo R), se identifican (4) las diagonales y sus puntos iniciales (representantes de equivalencia), y finalmente se gira (5) el eje de ordenadas, en un ángulo de noventa grados hacia la izquierda, hasta obtener la recta discreta $\mathbb{Z}$. La limpieza geométrica de la construcción refleja la gran armonía de la invención matemática. Un hecho importante que *no* alcanza a detectarse en los diagramas es el buen enlace («congruencia») entre las operaciones aritméticas y las representaciones geométricas de las clases de equivalencia.



8.2. Más sobre divisibilidad en $\mathbb{Z}$

A lo largo de este texto, desde el sorprendente diagrama de Hasse de la divisibilidad en $\mathbb{N}$ (capítulo 1), hemos venido estudiando ciertas propiedades de la relación de divisibilidad. Si *ampliamos* el universo de la relación de divisibilidad al conjunto de los enteros (con la misma definición usual: $a \mid b$ si y sólo si $\exists m \in \mathbb{Z}(b = ma)$), podemos encontrar *nuevas* relaciones de gran interés que no podían ser expresadas sólo en el universo de los naturales.

Dados $a, b \in \mathbb{Z}$, el máximo común divisor (*mcd*) de a y b se define mediante las condiciones: (i) $mcd(a,b) \in \mathbb{N}$ (ii) $mcd(a,b) \mid a$, $mcd(a,b) \mid b$; (iii) si $d' \mid a$ y $d' \mid b$ entonces $d' \mid mcd(a,b)$ (compárese con la situación en el ejemplo 5.4, donde el *mcd* se había definido para m y n naturales). Un hecho de incalculable importancia para el desarrollo posterior de la aritmética ocurre entonces en $\mathbb{Z}$.

Teorema 8.5. *Identidad de Bézout.*[1] *Para todos $a, b \in \mathbb{Z}$ existen $x, y \in \mathbb{Z}$ tales que $mcd(a,b)=ax+by$. De esta manera, el máximo común divisor es una combinación lineal en $\mathbb{Z}$.*

Demostración. Observe primero que la identidad no va a poder conseguirse en el conjunto $\mathbb{N}$: $mcd(3,5) = 1 \neq 3x+5y$ si restringimos x, y a los naturales. En el ámbito ampliado $\mathbb{Z}$, sí se conseguirá en cambio la identidad: el conjunto $\mathbb{Z}$ estará cumpliendo a la perfección con el cometido de ayudar a resolver combinaciones lineales más complejas. La prueba del teorema es extremadamente instructiva pues para demostrar una propiedad *específica* de $\mathbb{Z}$, se trasladará la prueba a una problemática *específica* de $\mathbb{N}$. La *transferencia* de ciertas condiciones en un ámbito matemático a *otras* condiciones en otro ámbito, con la consiguiente resolución (al menos parcial) de la problemática original, es un proceso profundo, propio de la matemática moderna. Se trata de algo que el estudiante recorrerá posteriormente en cursos como TEORÍA DE GALOIS, TOPOLOGÍA ALGEBRAICA, TEORÍA DE CATEGORÍAS o ANÁLISIS FUNCIONAL.

---

1 Étienne Bézout (Francia, 1730-1783) escribió varios volúmenes de matemáticas para el uso de la artillería francesa, y un importante tratado póstumo sobre las ecuaciones algebraicas.

Sean entonces $a, b \in \mathbb{Z}$. Si $a = b = 0$ entonces $mcd(a,b) = 0$, y 0 es una combinación lineal de la manera más fuerte posible: $0 = 0x + 0y$ para *cualesquiera* x, y. Podemos asumir entonces que $a \neq 0$ o $b \neq 0$. Considere el conjunto $L = \{ax + by : ax + by > 0\ ,\ x, y \in \mathbb{Z}\}$ (conjunto de las combinaciones lineales *estrictamente positivas* de a y b con coeficientes en $\mathbb{Z}$). Por construcción, $L \subseteq \mathbb{N}$ (nos hemos *transferido* por tanto hacia los naturales). Es fácil ver que L no es vacío, es decir que existe al menos una de esas combinaciones lineales que es estrictamente positiva: suponiendo, por ejemplo, que $a \neq 0$, si $a > 0$ se tiene que $a \cdot 1 + b \cdot 0 = a$ es combinación lineal estrictamente positiva, y si $a < 0$ se tiene que $a \cdot (-1) + b \cdot 0 = -a$ es combinación lineal estrictamente positiva. Como L es un conjunto *no vacío* de naturales, el *buen orden* en $\mathbb{N}$ (sección 7.3) nos asegura que L posee un mínimo elemento d ($d \in L$: esto es fundamental en el buen orden). Vamos a demostrar que obligatoriamente $d = mcd(a,b)$, por lo tanto el *mcd* estará en L (pues $d \in L$) y será así una combinación lineal de a y de b, como deseado.

Como $d \in L \subseteq \mathbb{N}$, d es natural, y se cumple la primera condición para el *mcd* en $\mathbb{Z}$. Para la segunda condición, debemos asumir como conocido (en el colegio: si no es el caso, un instructor del curso podrá probarlo) el **algoritmo de división de Euclides**[2]:

para $m, n \in \mathbb{Z}$ existen $q, r \in \mathbb{N}$ tales que $m = nq + r$ con $0 \leq r < |n|$.

Veamos entonces que $d \mid a$ (de forma similar se obtiene $d \mid b$). Procedemos *por contradicción*: suponga que $d \nmid a$; entonces, en la división euclidiana de a por d, el resto de la división *no es nulo*: tenemos que $a = dq + r$ con $0 < r < d$. Se deduce $r = a - dq = a - (ax + by)q$ (recuérdese que $d \in L$, por tanto $d = ax + by$ para adecuados x, y), de donde $r = (1 - xq)a + (-yq)b$. *Como además* $r > 0$ (esto es esencial), se tiene que $r \in L$. Pero aquí llegamos a la contradicción deseada porque $r < d$ contradice la definición de d como *mínimo elemento* de L.

Nos queda finalmente por verificar la tercera condición del *mcd*. Ésta resulta ser inmediata gracias a la expresión de d como combinación lineal.

---

2 Euclides (Grecia, siglo III a.C.) es el prototipo del gran matemático de la antigüedad. Los *Elementos* de Euclides constituyeron el paradigma de un cuerpo de demostraciones en matemáticas por más de dos mil años, hasta el advenimiento de las geometrías no euclidianas (Gauss, Bolyai, Lobachevski, Riemann) en el siglo XIX.

En efecto, suponga que $d' \mid a$ y $d' \mid b$; entonces $d' \mid ax + by = d$. □

Un análisis de la prueba anterior es iluminador. Se involucran en la demostración *múltiples estratos* matemáticos y lógicos: propiedades de divisibilidad, algoritmo de división, intercambios muy cuidadosos entre $\mathbb{Z}$ y $\mathbb{N}$, fuerza del buen orden en $\mathbb{N}$, pruebas directas, subpruebas por contradicción, etc. *La riqueza de enlaces entre esos diversos estratos es característica de la matemática*, cuando ésta empieza a expresar resultados de un considerable interés *mixto*, tanto metodológico, como conceptual.

La prueba que hemos dado de la identidad de Bézout es una prueba con un gran contenido estructural, pero, en principio, se trata sólo de un teorema de existencia: dados $a, b \in \mathbb{Z}$ el teorema nos asegura que existen $x, y \in \mathbb{Z}$ tales que $mcd(a, b) = ax + by$, pero no nos dice cuáles podrían ser esos números. Sin embargo, un «deshilvanamiento recursivo» del algoritmo de división de Euclides proporciona *de manera efectiva* los coeficientes x, y tales que $mcd(a, b) = ax + by$. Sea, por ejemplo, a encontrar $x, y \in \mathbb{Z}$ tales que $1 = 11x + 30y$ (existirán pues $1 = mcd(11, 30)$). Divida 30 por 11 según el algoritmo de Euclides: $30 = 11 \times 2 + 8$; divida 11 por 8: $11 = 8 \times 1 + 3$; divida 8 por 3: $8 = 3 \times 2 + 2$; divida 3 por 2: $3 = 2 \times 1 + 1$; divida 2 por 1: $2 = 2 \times 1 + 0$. De esta manera, dividiendo cocientes por restos, en algún momento se llegará a 0 (¿por qué?); el *anterior resto no nulo* será el *mcd*, pero, mejor aún, deshilvanando la información obtenida en las diversas divisiones, podrá reconstruirse al *mcd* como la combinación deseada. En efecto, $1 = 3 - 2 \times 1 = 3 - (8 - 3 \times 2) \times 1 = 3 \times 3 - 8 = (11 - 8) \times 3 - 8 = 11 \times 3 - 8 \times 4 = 11 \times 3 - (30 - 11 \times 2) \times 4 = 11 \times 11 - 30 \times 4$, por tanto $x = 11$ y $y = -4$. Este proceso proporciona una solución posible; en realidad, siempre hay *infinitas* soluciones (en enteros x, y) para la ecuación (ejercicio 8.4).

Algunas relaciones de equivalencia de gran utilidad en $\mathbb{Z}$ son las congruencias módulo n ($n \in \mathbb{N}$).

Definición 8.6. Sea $n \in \mathbb{N}$. Para $a, b \in \mathbb{Z}$, definimos $a \equiv_n b$ si y sólo si $n \mid a - b$ (esto debe leerse: «a es congruente con b módulo n»).

El caso $n = 0$ corresponde a la igualdad, pues $a \equiv_0 b$ si y sólo si $0 \mid a - b$ si y sólo si $a - b = 0$ si y sólo si $a = b$. El caso $n = 1$ no proporciona ninguna información interesante, pues $a \equiv_1 b$ para *todos* $a, b \in \mathbb{Z}$. En cambio, para $n \geq 2$ las congruencias codifican una enorme cantidad de información aritmética. Es fácil verificar que estas relaciones son relaciones de equivalencia, pero, mejor aún, son relaciones que se comportan bien con respecto a

la suma y la multiplicación (como sucedía con la relación R que nos permitió construir al conjunto de los enteros). Tenemos en efecto (ejercicio 8.3):

$$a \equiv_n b\ ,\ c \equiv_n d \ \rightarrow\ a+c \equiv_n b+d\ ,\ ac \equiv_n bd.$$

Las relaciones de congruencia $\equiv_n$ están íntimamente ligadas a los subconjuntos $n\mathbb{Z}$, pues $a \equiv_n b$ equivale a decir $a - b \in n\mathbb{Z}$. En cursos posteriores (ÁLGEBRA ABSTRACTA, ÁLGEBRA UNIVERSAL, TEORÍA DE CATEGORÍAS) el estudiante descubrirá que éste es un caso particular de situaciones profundas mucho más generales (correspondencia entre «núcleos» y «congruencias»).

El *buen comportamiento* de las congruencias $\equiv_n$ con respecto a las operaciones es la base para realizar cómodos cálculos que serían bastante más engorrosos sin las congruencias. Por ejemplo, el cálculo del resto de la división de 3^{98} por 5 se obtiene fácilmente (habiendo demostrado el ejercicio 8.3) mediante las congruencias módulo 5: $3^{98} = (3^2)^{49} = 9^{49} \equiv_5 (-1)^{40} = -1 \equiv_5 4$. Así, se ve fácilmente que el resto buscado es igual a 4. Pero imagine realizar la división calculando explícitamente 3^{98}: ¡no existirían suficientes átomos en el universo para efectuar un tal cálculo!

El cálculo anterior codifica en un ejemplo particular una de las *razones de ser* primordiales de las congruencias: simplificar cálculos multiplicativos grandes (algo que se conseguirá también con los logaritmos de números reales, ver final de la sección 11.1). De hecho, cada potencia de la forma a^{nm} se expresa como $(a^n)^m$ (sin usar congruencias), y, usando ahora sí congruencias, se *reduce primero* a^n módulo la congruencia deseada, para *luego* tomar la potencia m-ésima. En ciertos casos particulares (congruencias módulo un número *primo* p), las potencias adquieren una expresión especialmente sencilla, y *siempre* se tiene $a^p \equiv_p a$ para todo $a \in \mathbb{Z}$ (no demostraremos esto aquí; para un caso particular, véase el ejercicio 8.7). Vía las congruencias, las potencias módulo un primo adquieren entonces un comportamiento «cíclico», pues éstas empiezan a repetirse ($a^{p+1} = a^p a \equiv_p aa = a^2$, y, en general, $a^{p+i} \equiv_p a^{i+1}$ si $1 \leq i < p$). El estudio *general* de esas estructuras cíclicas lleva a los comienzos de un curso posterior de ÁLGEBRA ABSTRACTA.

8.3. Números racionales

El interés de los argumentos de divisibilidad en los enteros *desaparece* si entramos al mundo de los racionales, donde *todos* los números (excepto 0) se dividen unos a otros. No obstante, el «completamiento» de los enteros con respecto a la relación de divisibilidad da lugar a un extenso universo de

números, esencialmente valioso como ámbito para realizar *aproximaciones construibles* infinitamente pequeñas entre los números. Se *abre* así un espacio de aproximación hacia lo infinitesimal, que se *cerrará* luego (en una primera instancia) con los números reales (próximo capítulo).

La construcción de los números racionales a partir de los enteros procede metodológicamente de la misma manera como los enteros se construyeron a partir de los naturales:

$$\mathbb{N} \dashrightarrow \mathbb{Z}:$$

construcción de inversos para la suma $(+)$, vía clases de equivalencia

$$(a,b)R(c,d) \leftrightarrow a+d=b+c \ (a,b,c,d \in \mathbb{N});$$

$$\mathbb{Z} \dashrightarrow \mathbb{Q}:$$

construcción de inversos para la multiplicación $(\cdot)$, vía clases de equivalenci

$$(a,b)S(c,d) \leftrightarrow ad=bc \ (a,b,c,d \in \mathbb{Z}, b \neq 0 \neq d).$$

La idea consiste en identificar todas las representaciones del tipo $\frac{a}{b}$, donde $b \neq 0$: el tener $\frac{a}{b} = \frac{c}{d}$ obliga a cumplir la relación $ad = bc$, es decir a que las parejas (a,b) y (c,d) estén en S. Se demuestra (ejercicio 8.8) que esta nueva relación S es también una relación de equivalencia. $\mathbb{Q}$ se define entonces como el conjunto de las clases de equivalencia de S.

Definición 8.7. El conjunto de los números racionales $\mathbb{Q}$ se define por:

$$\mathbb{Q} = \{[(a,b)]_S : (a,b) \in \mathbb{Z} \times \mathbb{Z}, b \neq 0\}.$$

Las operaciones de suma y multiplicación en $\mathbb{Q}$ se definen por:

$$[(a,b)]_S + [(c,d)]_S = [(ad+bc, bd)]_S$$

$$[(a,b)]_S \cdot [(c,d)]_S = [(ac, bd)]_S.$$

Las nuevas operaciones definidas en $\mathbb{Q}$ se comportan bien con respecto a S (es decir, S es una «congruencia»: ver ejercicio 8.8). Compárese esta definición con la definición (8.4) de suma y multiplicación entre enteros: para $\mathbb{Z}$, la suma (entre clases de equivalencia) es obvia y la multiplicación es delicada; en cambio, para $\mathbb{Q}$ la multiplicación es obvia y la suma más delicada. Esto es razonable, puesto que las modificaciones que se hacen en una de las dos operaciones tienden a afectar más a su contraparte que a ella misma.

La notación usual para racionales consiste en escribir $[(a,b)]_S = \frac{a}{b}$ y en identificar $[(a,1)]_S$ con a (para $a \in \mathbb{Z}$), mediante la inyección $\mathbb{Z} \longrightarrow \mathbb{Q} : a \mapsto [(a,1)]_S$. El hecho fundamental conseguido con los racionales consiste en contar entonces con inversos para la multiplicación: si $a \neq 0 \neq b$,

$$\frac{a}{b} \cdot \frac{b}{a} = [(a,b)]_S \cdot [(b,a)]_S = [(ab,ba)]_S = [(1,1)]_S = 1.$$

Detrás de las igualdades entre clases de equivalencia yacen, ya sea notaciones sencillas, ya sea propiedades profundas de los conjuntos de números: por ejemplo, la penúltima igualdad en la línea anterior se debe a la conmutatividad de la multiplicación en $\mathbb{Z}$ y al hecho de que 1 actúa como neutro para la multiplicación. De esta manera se *enlazan* constantemente propiedades de un ente matemático en un nivel dado, y nuevas propiedades de nuevos entes en un nivel de complejidad mayor: se trata de una profunda *recursividad arquitectónica* en el mundo de las matemáticas.

Las propiedades (A1)-(A5) que se tenían para las operaciones de suma y multiplicación entre enteros (incluida la existencia de inversos aditivos) siguen satisfaciéndose para racionales. La ganancia aquí obtenida consiste en una «ampliación» o «compleción» de la parte multiplicativa del axioma (A3), gracias a los inversos para la multiplicación:

$$\forall \frac{a}{b} \in \mathbb{Q}(a \neq 0) \;\; \exists \frac{c}{d} \in \mathbb{Q} \;\; \frac{a}{b} \cdot \frac{c}{d} = 1.$$

Fallan ahora, en cambio, tanto el orden usual capaz de ser capturado mediante la suma (A6), como el principio de inducción (Ind). El objetivo de los racionales consiste en proveer una buena aproximación a lo infinitamente pequeño, como veremos en el próximo capítulo; se gana doblemente, al obtener inversos para la suma y la multiplicación (lo que nos llevará a lo infinitamente pequeño), pero se pierde también doblemente en lo que respecta al orden inductivo y «granulado» de los naturales. Esto es algo fundamental en el mundo de las matemáticas: *dependiendo de qué problemáticas* deseen abordarse, ciertas estructuras matemáticas se encuentran mejor adaptadas que otras para enfocar esas problemáticas. Una diversidad de problemas lleva a una diversidad de estructuras, y el estudiante de matemáticas debe estar saltando constantemente de una estructura a otra.

En $\mathbb{Q}$ se define un orden de la manera esperada, mediante $\frac{a}{b} \leq \frac{c}{d} \leftrightarrow ad \leq bc$ en el caso $a,b,c,d \in \mathbb{N}$, y mediante las modificaciones adecuadas (¿cuáles?) en el caso negativo. Este nuevo orden que se obtiene en $\mathbb{Q}$ posee

una propiedad muy importante que codifica en buena medida la *especificidad* de los racionales ($<$ denota el orden *estricto*, $x < y \leftrightarrow x \leq y \wedge x \neq y$):

$$\forall \frac{a}{b} < \frac{c}{d} \in \mathbb{Q} \ \exists \frac{e}{f} \in \mathbb{Q} \ \ \frac{a}{b} < \frac{e}{f} < \frac{c}{d}.$$

De hecho, en el caso $\frac{a}{b} > 0$, basta con tomar $\frac{e}{f} = \frac{a+c}{b+d}$ (chequéelol) y, en el caso negativo, una modificación adecuada (¿cuál?). Resulta así que el orden de los racionales es denso: entre un par de números distintos, existe al menos otro número. En realidad, existen entonces infinitos números entre ellos (ejercicio 8.9), y todo intervalo (no trivial) $[\frac{a}{b}, \frac{c}{d}]$ de racionales es *infinito*. Se trata, por supuesto, de una notable diferencia con los intervalos de enteros o de naturales $[m, n]$ que, en cambio, son *siempre finitos*.

8.4. Ejercicios

8.1. Sea A un conjunto no vacío. Sea $\mathcal{R}$ el conjunto de las relaciones de equivalencia sobre A, y sea $\mathcal{P}$ el conjunto de las particiones de A. Demuestre que la correspondencia $F : \mathcal{R} \longrightarrow \mathcal{P}$, que envía una relación de equivalencia en la partición de las clases de equivalencia de esa relación, es biyectiva. Ayuda: explicite una correspondencia $G : \mathcal{P} \longrightarrow \mathcal{R}$ que asocie una relación de equivalencia a una partición (la idea aparece en el cuerpo del texto), y demuestre que las funciones F y G son inversas la una de la otra.

8.2. Sea R la relación en $\mathbb{N} \times \mathbb{N}$ definida en el ejemplo 8.3. Demuestre que la suma entre enteros (entendidos como clases de equivalencia bajo R) es *independiente de los representantes* de las clases, es decir, demuestre que si $[(a,b)]_R = [(a',b')]_R$ y $[(c,d)]_R = [(c',d')]_R$ entonces $[(a+c, b+d)]_R = [(a'+c', b'+d')]_R$. Muestre también que la multiplicación es independiente de los representantes: escriba la frase adecuada que expresa esa independencia y demuéstrela.

8.3. Sean $a, b, c, d \in \mathbb{Z}$. Demuestre que $a \equiv_n b$ y $c \equiv_n d$ implica $a+c \equiv_n b+d$ y $ac \equiv_n bd$. Deduzca que $a \equiv_n b$ implica $a^j \equiv_n b^j$ para todo $j \in \mathbb{N}$ (esto es, las congruencias preservan potencias).

8.4. Demuestre que la identidad de Bézout posee infinitas soluciones (dados $a, b \in \mathbb{Z}$ existen infinitos $x, y \in \mathbb{Z}$ tales que $mcd(a,b) = ax + by$). Ayuda: combine *una* solución de la identidad de Bézout con *infinitas* soluciones (fáciles, búsquelas) para la ecuación $at + bz = 0$.

8.5. Encuentre explícitamente $x_1, y_1, x_2, y_2, x_3, y_3 \in \mathbb{Z}$ tales que:

$$3 = 21x_1 + 15y_1$$

$$1 = 33x_2 + 35y_2$$

$$72 = 2880x_3 + 504y_3.$$

8.6. Encuentre $a \in \mathbb{Z}$ tal que $a \equiv_{33} 10$ y $a \equiv_{35} 7$ (*simultáneamente*). Ayuda: calcule la expresión lineal del $mcd(33, 35)$ y con modificaciones adecuadas resuelva las ecuaciones $a = 10 + 33k = 7 + 35k'$.

8.7. Calcule 3^6 (módulo 7), 4^6 (módulo 7), 5^6 (módulo 7). ¿Puede intuir una fórmula general detrás de estos casos particulares? ¿Puede probarla?

8.8. Sea S la relación en $\mathbb{Z}\times\mathbb{Z}$ introducida antes de la definición 8.7. Demuestre que S es una congruencia, es decir (i) S es relación de equivalencia; (ii) S preserva suma y multiplicación: si $[(a,b)]_S = [(a',b')]_S$ y $[(c,d)]_S = [(c',d')]_S$ entonces $[(ad + bc, bd)]_S = [(a'd' + b'c', b'd')]_S$; si $[(a,b)]_S = [(a',b')]_S$ y $[(c,d)]_S = [(c',d')]_S$ entonces $[(ac,bd)]_S = [(a'c', b'd')]_S$.

8.9 Sean $\frac{a}{b} < \frac{c}{d} \in \mathbb{Q}$. Demuestre que existen infinitos racionales entre $\frac{a}{b}$ y $\frac{c}{d}$. Ayuda: hágalo primero para el caso positivo, verificando la construcción sugerida de *un* racional estrictamente metido en el intervalo y *repitiendo* infinitamente el proceso; luego, extienda la situación al caso negativo.

Capítulo 9

Números reales

Contenido

9.1. Sucesiones de racionales 94
9.2. Vecindades fundamentales 96
9.3. Completamiento de los racionales 98
9.4. Propiedades fundamentales de los reales 99
9.5. Ejercicios 103

Los números reales constituyen una suerte de primer *ascenso considerable* para el estudiante que entra en la Carrera de Matemáticas. En el universo de los reales muchas de las propiedades básicas de los conjuntos de números subyacentes ($\mathbb{N}, \mathbb{Z}, \mathbb{Q}$) adquieren un *nuevo relieve*. Por su simple posicionamiento en un universo *no enumerable*, mucho más rico, esas propiedades pasan a servir de nuevos peldaños *parciales* en la comprensión de los difíciles fenómenos de trascendencia que caracterizan a los reales. Con el conjunto de los números reales, el estudiante de la Carrera de Matemáticas tiene a su disposición un *primer modelo del continuo* que no dejará de aparecer y de sorprenderle en sus estudios posteriores.

9.1. Sucesiones de racionales

Como hemos visto en la sección 8.3, el orden de los racionales es denso (¿podría intentar *dibujar* ese orden?), pero como también sabemos desde el capítulo 1, se trata de un orden con «huecos» (irracionalidad de $\sqrt{2}$), y,

en realidad, con infinitos «huecos» (infinitos irracionales, ejercicio 3.2). Más aún, si manejamos por ahora intuitivamente la idea de que el conjunto de números reales $\mathbb{R}$ puede verse como la unión $\mathbb{Q} \cup \mathbb{I}$ de racionales e irracionales, como sabemos que $\mathbb{Q}$ es enumerable y que $\mathbb{R}$ no lo es, se sigue que $\mathbb{I}$ no es enumerable: hay muchísimos más irracionales que racionales. Entonces, el orden de los racionales, aunque es denso, está sin embargo literalmente «repleto de huecos». La (infinita) *subsanación* de esos huecos, *pegando* entre sí todos los números, va a dar lugar al conjunto de los números reales.

Para «cubrir» esos huecos, una idea natural (debida a Cantor) consiste en acumular colecciones de racionales, pegándolas progresivamente, a medida que los racionales se acercan entre sí. Para ello, necesitamos precisar qué son esas colecciones de racionales (esta sección), qué noción de cercanía puede cobijarlas (sección 9.2) y cómo podemos luego pegarlas adecuadamente (sección 9.3). Otra idea distinta, debida a Dedekind[1], consiste en considerar ciertos subconjuntos de racionales («cortaduras» de Dedekind) como los objetos mismos que cubrirán los huecos. Las dos aproximaciones son equivalentes (Cantor y Dedekind intercambiaron de hecho una extensa correspondencia alrededor del nacimiento de la teoría de conjuntos), pero no exploraremos aquí la visión de Dedekind.

Definición 9.1. Una **sucesión** de racionales es una función $s : \mathbb{N} \longrightarrow \mathbb{Q}$ (más generalmente, una sucesión de elementos en un conjunto A es una función $\mathbb{N} \longrightarrow A$). La función s se puede identificar con la colección de las imágenes de s: $s(0), s(1), s(2), \ldots, s(n), \ldots$ Para mayor comodidad en la escritura, la sucesión se denota mediante subíndices: $(s_0, s_1, s_2, \ldots, s_n, \ldots)$, en forma extensa, o también $(s_n)_{n\geq 0}$, o sencillamente $(s_n)_n$, en forma compacta. s_n se llama el n-ésimo término de la sucesión s.

Ejemplo 9.2. Las siguientes son sucesiones de racionales:

$(1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots)$; se tiene $s_n = \frac{1}{n+1}$.

(1,1.4,1.41, 1.414, 1.4142, 1.41421, ...); se tiene s_n= expansión decimal de $\sqrt{2}$ con n décimas.

---

[1] Richard Dedekind (Alemania, 1831-1916) es uno de los padres de las matemáticas modernas. Sus aportes en teoría de números antecedieron la eclosión posterior del álgebra abstracta. La profunda influencia de una aproximación *estructural* a las matemáticas nace con la obra de Dedekind.

$(1{,}2{,}2.5{,}\ldots, 1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!},\ldots)$; se tiene s_n = expansión en serie de e con $n+1$ términos.

Informalmente por el momento, con los casos del ejemplo anterior, se intuye cómo los comportamientos de los términos n-ésimos de las sucesiones de racionales pueden ser extremadamente distintos: en el primer caso s_n se «aproxima» a 0 (natural), en el segundo caso s_n se «aproxima» a $\sqrt{2}$ (irracional, pero algebraico), en el tercer caso s_n se «aproxima» a e (no algebraico: un resultado difícil, obtenido con las mejores herramientas del análisis matemático a fines del siglo XIX - para la definición de algebraico véase el ejercicio 6.6). Así, el *abanico de cubrimientos* con sucesiones de racionales resulta ser extremadamente amplio.

9.2. Vecindades fundamentales

Procedemos a definir la noción de «aproximación» recién mencionada.

Definición 9.3. El **valor absoluto** entre racionales es la función

$$|\ |:\mathbb{Q}\longrightarrow\mathbb{Q}:x\mapsto|x|=\begin{cases}x, & x\geq 0;\\ -x, & x\leq 0.\end{cases}$$

La **distancia** $d(x,y)$ entre dos racionales x, y se define por

$$d(x,y)=|x-y|.$$

Una **vecindad fundamental** $V_\epsilon(x)$ para un «número cualquiera» x (donde $\epsilon\in\mathbb{Q}, \epsilon>0$) se define por

$$V_\epsilon(x)=]x-\epsilon, x+\epsilon[=\{y\in\mathbb{Q}: x-\epsilon<y<x+\epsilon\}.$$

$V_\epsilon(x)$ es el conjunto de los racionales cuya *distancia* a x es a lo sumo ϵ. Mientras más pequeño es ϵ, más se condensa la vecindad alrededor de x, y mejor puede medirse la «aproximación» o «pegamiento» de un número con otro. Este «número» x del cual se habla puede ser, por supuesto, un número racional, pero podría ser también un número ideal aún inexistente.

En la siguiente definición procedemos en forma intuitiva, entendiendo que los números («límites») a los que se hace mención en la definición pueden ser racionales, pero *pueden también formar parte de un conjunto más*

grande de números ideales: los números «reales» (el lector con talante filosófico querrá explorar cómo lo «ideal» se convierte aquí en «real», y cómo las oscilaciones pendulares de la matemática son también delicadas oscilaciones filosóficas). No procedemos aquí de forma totalmente rigurosa, puesto que ese tratamiento formará parte de un curso posterior de la Carrera de Matemáticas (ANÁLISIS). Sin embargo, la idea consiste en observar que no existen suficientes límites en el conjunto de los racionales, y en agregar entonces *todos los límites posibles*. Como los límites aún no tienen derecho formal de existencia (así como los negativos o los racionales no existían formalmente antes de construirlos), habría que introducir nuevos entes para poder *representar* esos límites. En este caso, esos nuevos entes son *clases de equivalencia* de sucesiones adecuadas de racionales que se «condensan» en el infinito (llamadas «sucesiones de Cauchy»[2]). Una diferencia profunda entre la introducción de las clases de equivalencia a nivel de $\mathbb{Z}$ o de $\mathbb{Q}$, y, ahora, a nivel de $\mathbb{R}$, es que estas últimas clases involucran un *manejo existencial no constructivo* del infinito. No insistiremos aquí sin embargo en estas cuestiones. El estudiante deberá tener cuidado con estas dificultades en el futuro.

Definición 9.4. Sea $(s_n)_n$ una sucesión de racionales. Sea l un «número» (racional, o ideal, en una eventual extensión de $\mathbb{Q}$). Decimos que l es un límite de la sucesión $(s_n)_n$ si y sólo si para toda vecindad fundamental de l, *a partir de algún subíndice* n_0 todos los elementos de la sucesión pertenecen a la vecindad. Intuitivamente, a partir de un cierto momento todos los elementos de la sucesión se agolpan en las vecindades fundamentales del límite. Formalmente, $\forall \epsilon > 0\ \exists n_o\ \forall n \geq n_0\ |s_n - l| < \epsilon$ (donde $\epsilon \in \mathbb{Q}, n, n_0 \in \mathbb{N}$). Los límites, cuando existen, son únicos (ejercicio 9.3), y podemos reemplazar el artículo indefinido «un» límite por «el» límite.

En el caso de que l sea el límite de la sucesión $(s_n)_n$, decimos que $(s_n)_n$ converge a l, y denotamos este hecho por

$$(s_n)_n \longrightarrow l,$$

---

2 Augustin-Louis Cauchy (Francia, 1789-1857) renovó el rigor del pensamiento matemático en el siglo XIX. Sus notables avances en la teoría de las funciones de variable compleja le otorgaron un impulso definitivo a la disciplina.

o también por

$$l = \lim s_n.$$

Ejemplo 9.5. Considere el conjunto A de los números con expansiones decimales: $A = \{a.a_1a_2\ldots a_n\ldots,\ a \in \mathbb{Z},\ a_n \in \{0,\ldots,9\},\ n \geq 1\}$. Más adelante, en cursos posteriores, una vez se haya fundamentado correctamente el conjunto de los reales, se podrá ver que $A = \mathbb{R}$, que los racionales son los elementos de A con expansiones decimales finitas o periódicas (es decir, con repeticiones de ciclos del tipo $a_ia_{i+1}\ldots a_{i+k}$, a partir de algún i), y que los irracionales son los elementos de A con expansiones no periódicas. Fijemos $\alpha \in A$, $\alpha = a.a_1a_2\ldots a_n\ldots$ Sea $(s_n)_n$ la sucesión de racionales definida por s_n= expansión decimal de α con n décimas, es decir, $s_0 = a$, $s_1 = a.a_1$, $s_2 = a.a_1a_2$, ..., $s_n = a.a_1a_2\ldots a_n$. Tenemos que $|s_n - \alpha| = |0.00\ldots0a_{n+1}a_{n+2}\ldots| < \frac{1}{10^n}$ (realice los casos $n = 0, 1, 2$ para convencerse del patrón general!). Con mayor razón, entonces, para $m \geq n$, tenemos $|s_m - \alpha| < \frac{1}{10^n}$, pues $|s_m - \alpha| < \frac{1}{10^m} \leq \frac{1}{10^n}$. Esto quiere decir que, *a partir de* $m \geq n$, todos los s_m pertenecen a la vecindad fundamental $V_{\frac{1}{10^n}}(\alpha)$. Si pudiésemos reemplazar los números $\epsilon > 0$ que aparecen en la definición del límite por números del tipo $\frac{1}{10^n}$, con lo anterior habríamos demostrado completamente que *lim* $s_n = \alpha$: todo número (racional o irracional) con expansión decimal resultaría ser así el límite de sus expansiones decimales finitas (racionales). El hecho de poder reemplazar la colección de vecindades fundamentales $\{V_\epsilon : \epsilon > 0\}$ por la *subcolección* de vecindades $\{V_{\frac{1}{10^n}} : n \in \mathbb{N}\}$ corresponde sin embargo a una propiedad adicional de los números reales la *arquimedianeidad* de $\mathbb{R}$ (ver sección 9.4).

9.3. Completamiento de los racionales

El problema fundamental con la convergencia de sucesiones de racionales es que éstas no siempre convergen a números racionales. Esto es claro, por ejemplo, en el segundo caso presentado en el ejemplo 9.2. No obstante, no sólo no es ésta una coyuntura inusual, sino que se trata de una *situación ubicua* en la arquitectónica de las matemáticas, donde ciertas estructuras incompletas deben tender a *saturarse* con respecto a ciertas propiedades. Así como los inversos de naturales para la suma no eran usualmente naturales (sólo el inverso aditivo del natural 0 es natural: algo ínfimo en $\mathbb{Z}$), y así como los inversos de enteros para la multiplicación no eran usualmente enteros (sólo los inversos multiplicativos de los enteros -1 y 1 son enteros algo ínfimo en $\mathbb{Q}$), aquí tampoco los límites de sucesiones de racionales son

usualmente racionales (sólo una cantidad enumerable de esos límites podrán ser racionales: algo ínfimo en $\mathbb{R}$). La inexistencia de ciertos números lleva, en una primera instancia correspondiente a la *no saturación* de la suma, a *construir* $\mathbb{Z}$, y, en una segunda instancia correspondiente a la *no saturación* de la multiplicación, a *construir* $\mathbb{Q}$. Ahora, cuando entran en juego los límites de sucesiones de racionales, otra inexistencia de números, correspondiente a la *no saturación* de los límites, lleva a *postular* la conveniencia de un cierto conjunto $\mathbb{R}$ que posea todos los límites de sucesiones de racionales. Una vez más, como lo hemos venido indicando desde el prefacio y a lo largo del texto, el *tránsito hacia el umbral de una negación* (la no saturación en este caso) abre las compuertas de la inventividad matemática.

Definición 9.6. Sea $A \subseteq \mathbb{Q}$. La **clausura** de A (notación $\overline{A}$) se define como el conjunto de límites de sucesiones con elementos en A: $\overline{A} = \{a : \exists (s_n)_n \text{ con } s_n \in A \ , \ a = \lim s_n\}$. Como lo hemos señalado en los comentarios anteriores, no necesariamente los elementos de $\overline{A}$ son racionales: son nuevos objetos ideales que «completan» a los racionales. Definimos entonces al conjunto de los números reales como la clausura de los racionales, es decir, como el conjunto de *todos los límites* de sucesiones de racionales:

$$\mathbb{R} = \overline{\mathbb{Q}}.$$

Como lo hemos indicado en la sección anterior, esta «definición» es más descriptiva y sugerente que rigurosa. Una elevación «bien fundamentada» de los reales como sucesiones de racionales *requiere* usar las sucesiones de Cauchy y clases de equivalencia entre ellas, pero no es el momento de realizar esa labor en un curso de FUNDAMENTOS (en la frase anterior utilizamos el término «elevación» en vez de «construcción», pues en realidad la elevación del edificio está lejos de poder ser *efectivamente construida*).

9.4. Propiedades fundamentales de los reales

El conjunto de los números reales preserva las buenas propiedades que venían de los racionales (axiomas (A1)-(A5) completados con inversos) y sigue sin cumplir los axiomas propios de los naturales (orden discreto, inducción). El orden de los reales extiende el orden de los racionales (y, en realidad, se trata de dos órdenes casi indistinguibles: véase el ejercicio 3.10). La propiedad fundamental que se gana con la aparición de los reales, y que define en buena medida la *especificidad* de $\mathbb{R}$, es una propiedad profunda de **continuidad**.

La idea intuitiva subyacente en la continuidad consiste en observar que, con los límites de sucesiones de racionales, se cubren *todos* los «huecos» que podían yacer en $\mathbb{Q}$. Otra manera de expresar esa continuidad consiste en afirmar:

(CONT) Toda función $f : \mathbb{R} \longrightarrow \mathbb{R}$ de grado 3 posee al menos una raíz $x_0 \in \mathbb{R}$ (donde f «de grado 3» significa $f(x) = ax^3+bx^2+cx+d$, $a, b, c, d \in \mathbb{R}$, $a \neq 0$, y x_0 «raíz» significa $f(x_0) = 0$).

Obsérvese que esta propiedad (CONT) no vale para los racionales: la función $f(x) = x^3-2$ no posee *ninguna* raíz en $\mathbb{Q}$, pues $f(x) = (x-\sqrt[3]{2})(x^2+x\sqrt[3]{2}+\sqrt[3]{4})$, y se tiene, por un lado, $\sqrt[3]{2} \notin \mathbb{Q}$, mientras que, por el otro lado, $x^2+x\sqrt[3]{2}+\sqrt[3]{4}$ siempre es estrictamente positivo para $x \in \mathbb{Q}$ (chequéelo!). Cuando introduzcamos las *gráficas* de funciones de variable real (capítulo 11), la propiedad (CONT) se expresará diciendo que toda gráfica de una función polinomial (capítulo 12) de grado 3 corta el eje real *al menos una vez*. El *corte* asegurado entre el eje y la gráfica se debe a la *continuidad geométrica* de los objetos matemáticos en juego.

Otra manera alternativa de expresar la continuidad es la siguiente:

(COMPL) Todo subconjunto no vacío de números reales que está acotado superiormente posee una mínima cota superior en $\mathbb{R}$.

Aquí, si $A \subseteq \mathbb{R}$, una *cota superior* de A es cualquier real $a_0 \in \mathbb{R}$ tal que $\forall a \in A\ a \leq a_0$, y una *mínima cota superior* de A es una cota superior a_0 de A tal que, para cualquier otra cota superior a' de A, $a_o \leq a'$. Las mínimas cotas superiores, si existen, son únicas (verifíquelo!), y podemos cambiar el artículo indefinido «una» mínima cota superior, por «la» mínima cota superior.

Esta forma de continuidad es una suerte de *completitud en el orden* (de allí el término (COMPL)). Obsérvese que el conjunto de los racionales tampoco verifica (COMPL): considerando el conjunto $A = \{1, 2, 2{,}5, \ldots, 1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!}, \ldots\} \subseteq \mathbb{Q}$, es fácil ver que A posee cota superior en $\mathbb{Q}$ (por ejemplo, 3 es una cota superior de A), pero *no posee* en cambio mínima cota superior en $\mathbb{Q}$, pues esa mínima cota superior es igual a $e \in \mathbf{I}$.

Los números reales permiten cubrir así todos los «huecos» provenientes del conjunto de los racionales, ya sea desde el punto de vista de la resolución de las ecuaciones de grado 3 (**CONT**) (lo que permitirá luego encontrar raíces para todas las ecuaciones de grado *impar*), ya sea desde el punto de vista de la completitud del orden (**COMPL**). Sin embargo, ciertas ecuaciones elementales siguen siendo irresolubles en $\mathbb{R}$, como la ecuación $x^2+1=0$. Esto nos llevará, al final de este curso, a la construcción de los números complejos. Una *enorme sorpresa* se producirá entonces: añadiéndole a los reales *solamente una* solución para la ecuación $x^2+1=0$ se tendrán *siempre* soluciones para *todas* las ecuaciones!

Dos subconjuntos *notables* de reales son el conjunto $\mathbb{Q}$ de los racionales y el conjunto $\mathbb{I}$ de los irracionales. Estos subconjuntos forman una *partición* de $\mathbb{R}$, pues $\mathbb{Q}\cup\mathbb{I}=\mathbb{R}$ y $\mathbb{Q}\cap\mathbb{I}=\emptyset$. Los subconjuntos se comportan de manera sencilla con respecto a las operaciones de suma y multiplicación (ejercicio 9.4):

$a\in\mathbb{Q}, b\in\mathbb{Q} \rightarrow a+b\in\mathbb{Q}$

$a\in\mathbb{Q}, b\in\mathbb{Q} \rightarrow ab\in\mathbb{Q}$

$a\in\mathbb{Q}, b\in\mathbb{I} \rightarrow a+b\in\mathbb{I}$

$a\in\mathbb{Q}, b\in\mathbb{I}, a\neq 0 \rightarrow ab\in\mathbb{I}.$

Pero, mejor aún, existe una profunda propiedad de *densidad*, tanto de racionales, como de irracionales, en el conjunto de los reales. Sean $a,b\in\mathbb{R}$ con $a<b$; el *intervalo abierto* de reales entre a y b es el conjunto $]a,b[=\{x\in\mathbb{R}: a<x<b\}$; tenemos entonces:

(**DENS**) $\qquad]a,b[\cap\mathbb{Q}\neq\emptyset \qquad]a,b[\cap\mathbb{I}\neq\emptyset.$

Así, *por más pequeño que sea* el intervalo $]a,b[$, este intervalo siempre posee números racionales e irracionales. Si se repite indefinidamente este proceso, se deduce que todo intervalo $]a,b[$ posee en realidad *infinitos* racionales e irracionales (ejercicio 9.6). La prueba de la propiedad de densidad (**DENS**) depende de otra propiedad esencial del conjunto de los números reales:

(**ARQUIM**) $\qquad \forall a,b\in\mathbb{R}\ (a,b>0\rightarrow\exists n\in\mathbb{N}\ na>b).$

Esta última propiedad se llama la *propiedad arquimedeana* de los reales, en honor a Arquímedes, quien fue el primero en utilizarla extensamente en sus cálculos sobre la aproximación infinita de figuras geométricas. La propiedad arquimedeana es una propiedad que *reduce* una problemática de infinitud a una aproximación finitaria (cómo pasar del «infinitamente pequeño» a al «infinitamente grande» b, en casos extremos, mediante sólo un número finito n de traslaciones). Al igual que otras propiedades que hemos encontrado a lo largo del curso, la *reducibilidad* de una problemática compleja a una elemental tiene enormes consecuencias para los desarrollos locales ligados a las nociones que estén en ese momento en juego[3].

Indiquemos ahora cómo (ARQUIM) implica (DENS). Sean $a < b \in \mathbb{R}$ y sea el intervalo $]a, b[$. Consideremos primero el caso en que a y b son racionales. Tomando $\frac{a+b}{2}$ tenemos que $\frac{a+b}{2} \in]a, b[\cap \mathbb{Q} \neq \emptyset$. Ahora, queremos encontrar un irracional en el intervalo $]a, b[$; considere $b - a > 0$: por la propiedad arquimedeana (ARQUIM), existe $n \in \mathbb{N}$ tal que $n(b - a) > \sqrt{2}$ (en vez de $\sqrt{2}$, puede tomarse aquí cualquier número que sepamos es irracional); de esa desigualdad se deduce inmediatamente $a < a + \frac{\sqrt{2}}{n} < b$ (observe, de paso, que el n otorgado por la propiedad arquimedeana no puede ser nunca 0), por tanto $a + \frac{\sqrt{2}}{n} \in]a, b[\cap \mathbb{I} \neq \emptyset$, usando las propiedades sobre suma y multiplicación de racionales con irracionales.

Consideremos ahora el caso en que a es racional y b es irracional (el caso a irracional y b racional se trata de la misma manera). Entonces $\frac{a+b}{2} \in \mathbb{I}$, e inmediatamente $\frac{a+b}{2} \in]a, b[\cap \mathbb{I} \neq \emptyset$. Para encontrar ahora un racional en $]a, b[$, se toma n tal que $n(b-a) > 1$ (ARQUIM), de donde $a < a + \frac{1}{n} < b$, y entonces $a + \frac{1}{n} \in]a, b[\cap \mathbb{Q} \neq \emptyset$. Finalmente, si a y b son ambos irracionales, tomando n tal que $n(b-a) > 1$ (ARQUIM), se tiene que $a + \frac{1}{n} \in]a, b[\cap \mathbb{I} \neq \emptyset$. Por otro lado, mostrar que existe un racional en $]a, b[$ es más delicado en este caso, y remitimos al estudiante a un ejercicio instructivo (9.5).

---

[3] Arquímedes (Grecia, siglo III a.C.) es el otro gran matemático de la antigüedad, al lado de Euclides. Arquímedes se adelantó a su época, y muchos de sus trabajos pueden verse, en retrospectiva, como precursores del cálculo diferencial e integral. La obra de Arquímedes, como toda la filosofía y la matemática griega, fue preservada en la Edad Media gracias a la gran actividad científica de los califatos árabes. Sin el mundo árabe, ahora tan equivocadamente vilipendiado, el mundo occidental tal como lo conocemos no habría existido.

9.5. Ejercicios

9.1. Considere la operación $\odot$ definida en $\mathbb{R}$ por $x \odot y = x + y - xy$. ¿Es $\odot$ asociativa? ¿Es $\odot$ conmutativa? ¿Posee elemento neutro? Demuestre sus respuestas.

9.2. Sea $L = \{x \in \mathbb{Q} : x^2 < 2\}$. Demuestre que L no tiene máximo (es decir, no existe $a \in L$ tal que $\forall x \in L\ x \leq a$) (ayuda: si $a^2 < 2$, construya $b \in \mathbb{Q}$ tal que $a^2 < b^2 < 2$). Muestre, en cambio, que L posee mínima cota superior en $\mathbb{R}$. ¿Cuál es esa mínima cota superior?

9.3. Demuestre que, cuando existen, los límites de una (misma) sucesión son únicos (es decir, si l=lim s_n y l'=lim s_n entonces $l = l'$).

9.4. Demuestre las propiedades de suma y multiplicación de racionales e irracionales, señaladas en la sección 9.4. Demuestre, en cambio, que nada se puede asegurar acerca de la suma o la multiplicación de irracionales.

9.5. Si a y b son ambos irracionales, con $a < b$, demuestre que existe un racional en $]a, b[$.

9.6. Sean $a, b \in \mathbb{R}$ con $a < b$; demuestre que $]a, b[$ posee *infinitos* racionales e irracionales.

9.7. Sean $a, b \in \mathbb{R}$ tales que $a^2 \geq b$. Demuestre que $\sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}}$ es racional si y sólo si $a^2 - b$ y $\frac{1}{2}(a + \sqrt{a^2 - b})$ son ambos cuadrados de racionales.

9.8. Sean $a, b, c \in \mathbb{Q}$. Demuestre que si $a\sqrt{2} + b\sqrt{3} + c\sqrt{5} = 0$ entonces $a = b = c = 0$ («independencia lineal» de $\sqrt{2}, \sqrt{3}, \sqrt{5}$ sobre $\mathbb{Q}$). ¿Es el resultado cierto si $a, b, c \in \mathbb{R}$?

9.9. Encuentre números racionales α y β tales que $\sqrt[3]{7 + 5\sqrt{2}} = \alpha + \beta\sqrt{2}$ («base de una extensión» de números cuadráticos sobre $\mathbb{Q}$).

9.10. Sea $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$. Demuestre que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ y que $\frac{1}{1-\sqrt{2}} \in \mathbb{Q}(\sqrt{2})$. Demuestre que $\mathbb{Q}(\sqrt{2})$ es *cerrado* bajo suma y multiplicación: $a, b \in \mathbb{Q}(\sqrt{2})$ implica $a + b, ab \in \mathbb{Q}(\sqrt{2})$.

9.11. La propiedad arquimedeana (una propiedad «geométrica») codifica, de manera esencial, ciertas propiedades de convergencia (propiedades «analíticas»). De hecho, demuestre la equivalencia plena:

(ARQUIM) si y sólo si $lim\frac{1}{n} = 0$.

Capítulo 10

Recapitulación sobre conjuntos de números

Contenido

10.1. Los conjuntos de números 105
10.2. El universo conjuntista 107
10.3. Ejercicios 109

En este capítulo proveemos una visión sintética, a vuelo de pájaro, sobre las diversas propiedades de los conjuntos que hemos visto hasta el momento (y que pronto veremos, adelantándonos a la aparición de los números complejos en los capítulos finales 13 y 14). Presentamos también una breve discusión del *universo conjuntista en expansión*, un muy extenso universo, «ancho y ajeno», que supera ampliamente los dominios de números usuales, alrededor de los cuales se concentra el curso de FUNDAMENTOS. Una vez más, observamos entonces que en el curso de FUNDAMENTOS nos encontramos apenas en la *punta de un iceberg*, cuya masa enorme y compleja escapa por el momento a nuestra mirada. Una de las maravillas de la matemática es su *inagotabilidad*, su inmensa riqueza que nunca alcanzamos a entender del todo, y que siempre nos impulsa a maravillarnos nuevamente con la gran creatividad del espíritu humano.

10.1. Los conjuntos de números

En la tabla siguiente presentamos en forma sucinta las principales propiedades de los conjuntos de números usuales (naturales, enteros, racionales, reales, complejos). Para referencia futura, dejamos constancia aquí de algunas propiedades del conjunto de los números complejos. El estudiante puede dejarlas de lado por el momento, y volver a ellas después de haber estudiado los capítulos 13 y 14.

propiedad	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
asociatividad $(+,\cdot)$	sí	sí	sí	sí	sí
conmutatividad $(+,\cdot)$	sí	sí	sí	sí	sí
distributividad ($\cdot$ sobre $+$)	sí	sí	sí	sí	sí
existencia neutros $(+,\cdot)$	sí	sí	sí	sí	sí
existencia inversos $(+)$	no	▶ sí	sí	sí	sí
existencia inversos $(\neq 0)$ $(\cdot)$	no	no	▶ sí	sí	sí
buen orden	▶ sí	no	no	no	no
existencia sucesor	sí	sí	no	no	no
densidad del orden	no	no	sí	sí	no
arquimedeaneidad del orden	sí	sí	sí	sí	no
«existencia de todo límite»	sí	sí	no	▶ sí	sí
existencia raíces «polinomios impares»	no	no	no	sí	sí
existencia raíces todo «polinomio»	no	no	no	no	▶ sí

Las frases y los términos entre comillas no han sido precisados con todo rigor. La «existencia de todo límite» se estudiará más adelante en la Carrera de Matemáticas (cursos de ANÁLISIS y de TEORÍA DE CONJUNTOS), aunque en el capítulo anterior se ha dado una primera introducción al tema. Aquí, al decir «existencia de todo límite», estamos pensando en la pertenencia (al conjunto dado) de todos los límites de sucesiones «razonables» de elementos de ese conjunto (técnicamente, esas sucesiones «razonables» son sucesiones de Cauchy: ver comentarios antes de la definición 9.4). Los «polinomios» se estudiarán también con más cuidado en cursos como ÁLGEBRA ABSTRACTA, ÁLGEBRA CONMUTATIVA o ESTRUCTURAS ALGEBRAICAS. No obstante, presentamos una breve introducción a los polinomios en el capítulo 12.

En la tabla anterior, denotamos con ▶ las *razones de ser* de cada conjunto de números: el interés de $\mathbb{N}$ radica en su buen orden, lo propio de $\mathbb{Z}$ es proveer inversos para la suma, lo propio de $\mathbb{Q}$ es proveer inversos para la multiplicación, el interés de $\mathbb{R}$ consiste en contener todos los límites de sucesiones de racionales, lo característico de $\mathbb{C}$ consiste en poder resolver todas las ecuaciones.

Los pasos esenciales codificados en la tabla anterior se resumen en las ampliaciones siguientes. Obsérvese cómo, en cada caso, *se supera una obstrucción*, ampliando el universo de los objetos matemáticos en juego:

$$\begin{array}{ccccccccc} \mathbb{N} & \rightsquigarrow & \mathbb{Z} & \rightsquigarrow & \mathbb{Q} & \rightsquigarrow & \mathbb{R} & \rightsquigarrow & \mathbb{C} \\ & \textit{inversos } (+) & & \textit{inversos } (\cdot) & & \textit{todo límite} & & \textit{toda raíz} & \end{array}$$

En particular, en el conjunto de los números complejos, se van acumulando muy buenas propiedades ligadas a una suerte de *completitud fuerte* (todos los límites, todas las raíces). No obstante, al acumular más y más entes «imaginarios» (en los complejos, la metáfora «imaginaria» se convertirá pronto en un objeto!), se *pierde* de manera definitiva el orden: como veremos, *no existe* en los complejos un orden «razonable», es decir que sea *congruente* con las operaciones de suma y multiplicación. Se trata de una *situación pendular*, típica de las matemáticas: lo que por un lado se gana, a menudo se pierde por otro lado. El matemático busca entonces encontrar las formas más ajustadas posibles de «equilibrio pendular» entre las diversas estructuras en juego.

Por otro lado, desde el punto de vista de los tamaños de infinitud, se tiene un claro salto de tamaño entre los conjuntos enumerables $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ (todos equipotentes a $\mathbb{N}$, como hemos visto) y el conjunto de los reales $\mathbb{R}$. De hecho, por el argumento diagonal de Cantor (4.15), $\mathbb{R}$ no es enumerable. Puede demostrarse que $\mathbb{R} \sim \wp(\mathbb{N})$, pues hay tantos reales como sucesiones de racionales, tantas sucesiones de racionales como sucesiones de naturales y tantas sucesiones de naturales como subconjuntos de naturales (para las precisiones, véase el ejercicio 10.3). La situación $\wp(\mathbb{N}) \sim \mathbb{R} \not\sim \mathbb{N}$ confirma el teorema de Cantor sobre los conjuntos potencia (4.14). Ahora bien, sabemos que el tamaño de $\wp(\mathbb{N})$ no es el mismo tamaño de $\mathbb{N}$, pero no sabemos qué tan grande puede ser en realidad $\wp(\mathbb{N})$ (por lo tanto, qué tan grande puede llegar a ser $\mathbb{R}$). Señalaremos en la próxima sección cómo ese tamaño puede ser *tan grande como se quiera*, tan infinitamente superior a $\mathbb{N}$ como se desee. Se trata de una *sorpresa mayúscula* en la matemática.

10.2. El universo conjuntista

Al empezar a explorar los conjuntos infinitos, Cantor construyó una *escala* de cardinales infinitos (llamados *alephs*), según la cual todo conjunto infinito debía poder ser medido en la escala. El hecho de que la escala resultara *completa*, y cubriera, en realidad, todos los tamaños infinitos, es un resultado delicado de la teoría de conjuntos, que requiere (y es de hecho equivalente) al *axioma de elección* (este axioma apareció subrepticiamente escondido en el ejercicio 4.15). Si escribimos la lista de los *alephs* como $\aleph_0, \aleph_1, \ldots, \aleph_n, \ldots$, y consideramos que $\aleph_0$, el primer tamaño de infinitud, es el tamaño de $\mathbb{N}$, resulta natural preguntarse acerca del tamaño de $\mathbb{R}$.

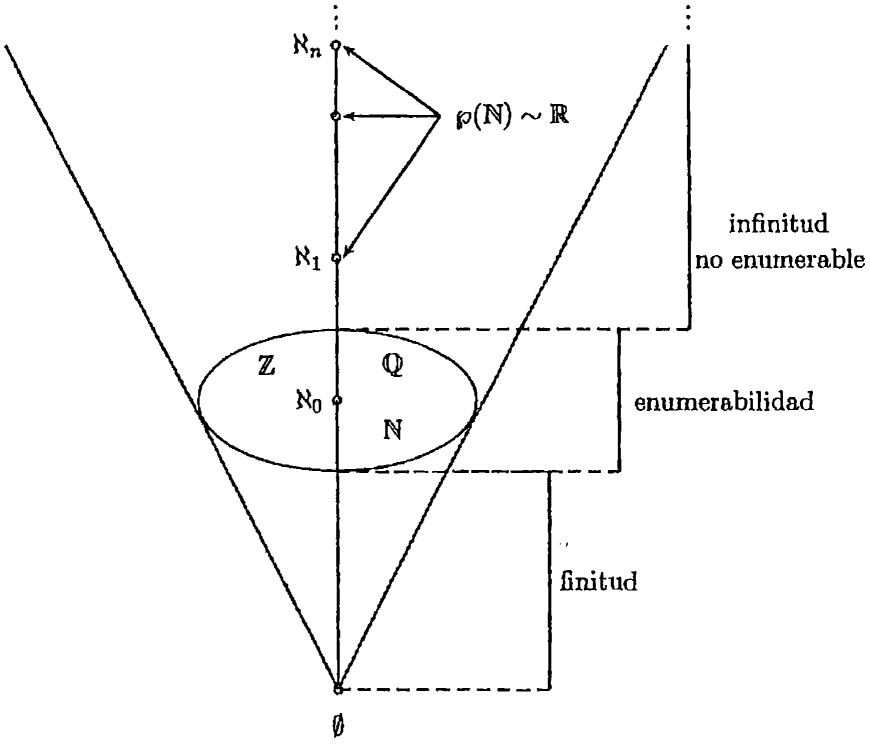
Cantor conjeturó que el tamaño del conjunto de los reales sería el *primer tamaño infinito después* del tamaño del conjunto de los naturales. Como el conjunto de los reales es un modelo del continuo, la conjetura de Cantor se denominó la **hipótesis del continuo**. En términos precisos, la hipótesis del continuo enuncia entonces que $\overline{\overline{\mathbb{R}}} = \aleph_1$ (la doble barra denota el cardinal de $\mathbb{R}$), donde $\aleph_1$ es el *primer cardinal no enumerable*. A pesar de enormes esfuerzos (que poco a poco debilitaron su salud, hasta llevarlo a una institución de enfermos mentales: peligros de la alta matemática!), Cantor no logró demostrar su hipótesis del continuo. En realidad, el problema era muy difícil, y *excedía* la técnica de la época (fines del siglo XIX y comienzos del XX). Un *comienzo* de solución del problema se obtuvo apenas en 1938 con Gödel, cuando éste demostró que *si el universo de conjuntos crece lentamente*, entonces la hipótesis del continuo es cierta. Pero surgió un sorpresivo *revés* de la situación, cuando Cohen[1] demostró en 1963 que, en otros universos de conjuntos cuyo *crecimiento es rápido*, el tamaño de los reales puede pasar a ser *cualquier* $\aleph_n$ ($n \in \mathbb{N}, n > 0$) (y, allende los $\aleph_n$, en escalas más altas de infinitud, sólo hay una mínima restricción para el tamaño de $\mathbb{R}$).

El universo de conjuntos puede entonces *variar* de formas bastante *erráticas*, y, *dependiendo del modelo* del universo que gustemos adoptar, podremos tener $\overline{\overline{\mathbb{R}}} = \aleph_n$ para *cualquier* $n \in \mathbb{N}, n > 0$. La situación es entonces

---

1 Paul Cohen (Estados Unidos, 1934-2007) revolucionó las pruebas de independencia en teoría de conjuntos, introduciendo su técnica del «forcing». Al *variar* los universos de la teoría de conjuntos, pueden forzarse sus propiedades, casi a gusto del observador.

lo más volátil posible: nada puede asegurarse, en principio, acerca del tamaño de $\mathbb{R}$. Los esfuerzos de los mayores matemáticos que trabajan en el área se dirigen entonces a buscar axiomas *naturales* adicionales que *fuercen* a situar el tamaño de $\mathbb{R}$ en un determinado nivel $\aleph_n$. Emergen así *múltiples teorías de conjuntos*, y el científico debe entonces escoger la teoría que más le convenga, de acuerdo con sus objetivos específicos.



En el diagrama, puede verse un universo conjuntista en expansión. Se parte del $\emptyset$, y se cubre en primera instancia el ámbito de los conjuntos finitos, mediante las operaciones $\wp$, $\cup$, $\cap$, $-$. Se llega luego a la enumerabilidad *postulando la existencia* de $\mathbb{N}$ (no hay modo de pasar de lo finito a lo infinito sin postular una infinitud). Siguiendo hacia adelante, gracias a la operación $\wp$, el teorema de Cantor (4.14) asegura que podemos superar lo enumerable. Mediante un buen comportamiento de las *funciones* («axioma de reemplazo») puede después *extenderse indefinidamente* el universo conjuntista, y puede accederse así a *alephs* cada vez más altos.

Los comportamientos de los objetos matemáticos dependen de su «encarnación» en esos universos conjuntistas en expansión. Así como se tienen múltiples teorías que, en formas alternativas, explican la evolución del cosmos a partir de un supuesto *big bang* inicial, múltiples teorías de conjuntos nos informan, con mayor o menor éxito, sobre el *elusivo* modelo del continuo conformado por los números reales. La teoría de modelos, debida a Tarski[2] y sus discípulos, se enlaza entonces de una manera muy fuerte con la teoría de conjuntos. Conocer en parte esos enlaces será una de las labores futuras de todo buen estudiante de la Carrera de Matemáticas.

10.3. Ejercicios

10.1. Confirme que usted conoce y maneja bien las propiedades de los conjuntos de números consignadas en la tabla de la sección 10.1.

10.2. Sea R una relación de orden en un conjunto A. Supóngase que esa relación R tiene un mínimo elemento m. Si $m \neq p \in A$, decimos que p es un átomo para R si no existe ningún otro elemento de A entre m y p (es decir, $\forall a \in A(mRa \wedge aRp \rightarrow a = m \vee a = p)$). Decimos que R es atómica si todo elemento de A (diferente del mínimo) posee al menos un átomo por debajo de él (es decir, $\forall a \in A - \{m\}$ $\exists p$ átomo pRa). Haga un diagrama de Hasse de lo que pretende definirse con la noción de átomo, y corrobore que esa noción se acopla bien con su intuición del término átomo. ¿Cuáles de las relaciones de orden usuales en los conjuntos de números $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ son atómicas? Muestre que la inclusión en $\wp(A)$ (para todo conjunto A no vacío) es atómica, y explicite cuáles son sus átomos. Muestre que la divisibilidad en $\mathbb{N}$ es atómica, y explicite cuáles son sus átomos.

10.3. Indicamos en este ejercicio cómo $\mathbb{R} \sim \wp(\mathbb{N})$. A lo largo del ejercicio, si A y B son dos conjuntos, A^B denota el conjunto de todas las funciones de B en A: $A^B = \{f : B \longrightarrow A: f \text{ es función}\}$.

---

2 Alfred Tarski (Polonia, 1902-1983) es uno de los lógicos matemáticos que más ha influido en el desarrollo de la disciplina en el siglo XX. La «teoría de modelos», fabricada en sus comienzos por Tarski y por su escuela, es la subrama actualmente más activa de la lógica, con sorprendentes aplicaciones en toda la matemática.

- Demuestre que $\wp(\mathbb{N}) \sim 2^{\mathbb{N}}$ (ayuda: dado $S \subseteq \mathbb{N}$, considere su función característica $\chi_S : \mathbb{N} \longrightarrow 2$ definida por $\chi_S(n) = 1$ si $n \in S$, y $\chi_S(n) = 0$ si $n \notin S$). Entendemos aquí 2 como el *conjunto* $2 = \{0, 1\}$ (definición conjuntista de 2). Por otro lado, en la sección 7.1, habíamos definido aritméticamente al *número* 2 mediante $2 = 1 + 1$; en un curso posterior de TEORÍA DE CONJUNTOS se mostrará que las dos definiciones (conjuntista y aritmética) *coinciden*.

- Demuestre que $2^{\mathbb{N}} \sim \mathbb{N}^{\mathbb{N}}$ (ayuda: exhiba una inyección de $\mathbb{N}^{\mathbb{N}}$ en $2^{\mathbb{N}}$, y use Schröder-Bernstein, sección 6.1).

- Demuestre que $\mathbb{Q}^{\mathbb{N}} \sim \mathbb{N}^{\mathbb{N}}$.

- Explique por qué se tiene $\mathbb{Q}^{\mathbb{N}} \sim \mathbb{R}$.

- Concluya de todo lo anterior que $\mathbb{R} \sim \wp(\mathbb{N})$.

10.4. El «axioma de elección» en teoría de conjuntos asegura que, dada una colección no vacía de conjuntos no vacíos, podemos elegir *simultáneamente* un elemento en cada uno de esos conjuntos no vacíos. Apoyándose explícitamente en el axioma de elección, muestre, ahora con algo más de rigor, que toda función sobreyectiva posee una inversa a derecha (ejercicio 4.15).

10.5. Sea A un conjunto no vacío. Una *función de elección* para A es una función $\phi : \wp(A) - \{\emptyset\} \longrightarrow A$ tal que $\phi(X) \in X$ para todo X, $\emptyset \neq X \subseteq A$. Describa explícitamente una función de elección para $A = \{1, 2, 3\}$. ¿Puede describir explícitamente una función de elección para $\mathbb{N}$ (fácil)? ¿Puede describir explícitamente una función de elección para $\mathbb{R}$ (difícil)? Muestre que una función de elección para A es 1-1 si y sólo si A posee un elemento.

10.6. (Continuación de 10.5). Demuestre que si existe una función de elección para A entonces toda función sobreyectiva con dominio A posee una inversa a derecha. La serie de ejercicios 4.15, 10.4 y 10.6 *precisa progresivamente* un concepto, hasta alcanzar un pleno rigor en el control de las pruebas. Es un proceso permanente en matemáticas, que el estudiante corroborará a lo largo de su Carrera.

10.7. Combinando el ejercicio 10.3 y la sección 10.2, vemos cómo la *exponenciación* cardinal infinita puede llegar a ser muy difícil de controlar ($2^{\aleph_0} = \aleph_1, \aleph_2, \ldots$ dependiendo del modelo del universo conjuntista en el que nos situemos). En cambio, la *suma* y la *multiplicación* cardinales en el infinito son «triviales»: (*) si A, B son conjuntos infinitos, $\overline{\overline{A}} + \overline{\overline{B}} = \overline{\overline{A}} \cdot \overline{\overline{B}} = max(\overline{\overline{A}}, \overline{\overline{B}})$.

No podemos aún demostrar este resultado general al nivel del curso de FUNDAMENTOS, pero, con las herramientas que tenemos disponibles, la prueba sí puede realizarse en un caso particular de enumerabilidad. Demuestre, por tanto, el caso particular de (*) para A enumerable, B infinito (no necesariamente enumerable): $\overline{\overline{A}} + \overline{\overline{B}} = \overline{\overline{A}} \cdot \overline{\overline{B}} = \overline{\overline{B}}$ $(= max(\overline{\overline{A}}, \overline{\overline{B}}))$. Ayudas: recuerde que B infinito significa que B posee un subconjunto enumerable (definición 3.1); use Schröder-Bernstein (sección 6.1); para el caso de la suma, use que unión de dos conjuntos enumerables es enumerable (ejercicio 6.5); para el caso del producto, use que un conjunto infinito contiene enumerables copias disyuntas de sí mismo.

Capítulo 11

Más sobre reales

Contenido

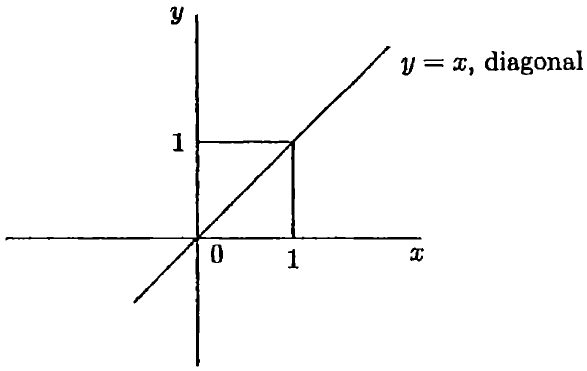
11.1. Gráficas de funciones 113
11.2. Algebraicidad y trascendencia 122
11.3. Ejercicios 125

En este capítulo proporcionamos algunas informaciones adicionales sobre el comportamiento de los números reales. En el capítulo 9, la construcción de los reales se realizó «internamente», completando los racionales *desde adentro*. En este capítulo, observamos en cambio a los reales *desde afuera*. El cambio de perspectiva corresponde a una dualidad ubicua, que da lugar a métodos y puntos de vista pendulares no sólo en matemáticas, sino en el ámbito más amplio de la epistemología y de la filosofía en general: la *dualidad de lo analítico versus lo sintético*. Un objeto (o concepto) matemático se define analíticamente a través de las propiedades de sus *constituyentes*. Un objeto (o concepto) matemático se define sintéticamente a través de sus propiedades con el *entorno*. Lo analítico se liga a la *descomposición*, lo sintético a la *composición*. En nuestro caso, los números reales se definieron analíticamente a través de las propiedades de completamiento de sus constituyentes fundamentales (sucesiones de racionales). En este capítulo, observamos en cambio algunas propiedades de los reales desde el punto de vista de las funciones que los transforman (sección 1), y desde el punto de vista de las ecuaciones que los describen (sección 2). La lectura funcional y la lectura ecuacional son perspectivas sintéticas que involucran la composición de funciones.

11.1. Gráficas de funciones

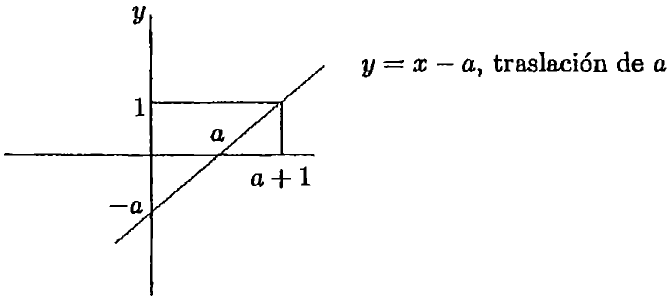
Presentamos a continuación diversas gráficas de funciones: (A) lineales; (B) cuadráticas; (C) cúbicas. Al final de la sección estudiamos parte del comportamiento *sintético* de estas gráficas.

A.1. Identidad: $id_{\mathbb{R}} : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x$



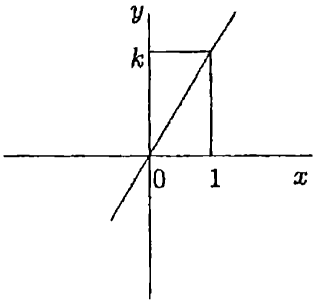
Un par de ejes (*abscisas*: x; *ordenadas*: y) proporciona una orientación del plano $\mathbb{R} \times \mathbb{R}$. Cada eje representa, con un *trazo continuo*, al conjunto $\mathbb{R}$. Cada diagrama representado en la retícula de los ejes será una *gráfica* de una función. En esta sección sólo consideraremos trazos continuos de funciones, sin huecos (sin «discontinuidades»). Algunos cursos posteriores de la Carrera (ANÁLISIS, TOPOLOGÍA, MEDIDA, ANÁLISIS FUNCIONAL) llevarán al estudiante a internarse en el riquísimo universo de las funciones discontinuas.

A.2. Traslación: $t_a : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x - a$



El diagrama representa el caso $a \geq 0$: se tiene una traslación a la derecha de la diagonal. Para el caso $a \leq 0$ se tendrá una traslación a izquierda de la diagonal. La «pendiente» de estas rectas sigue siendo la misma pendiente (=1) de la diagonal. Un movimiento Δx en las abscisas da lugar a un *mismo* movimiento $\Delta y = \Delta x$ en las ordenadas.

A.3. Homotecia: $h_k : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto kx$

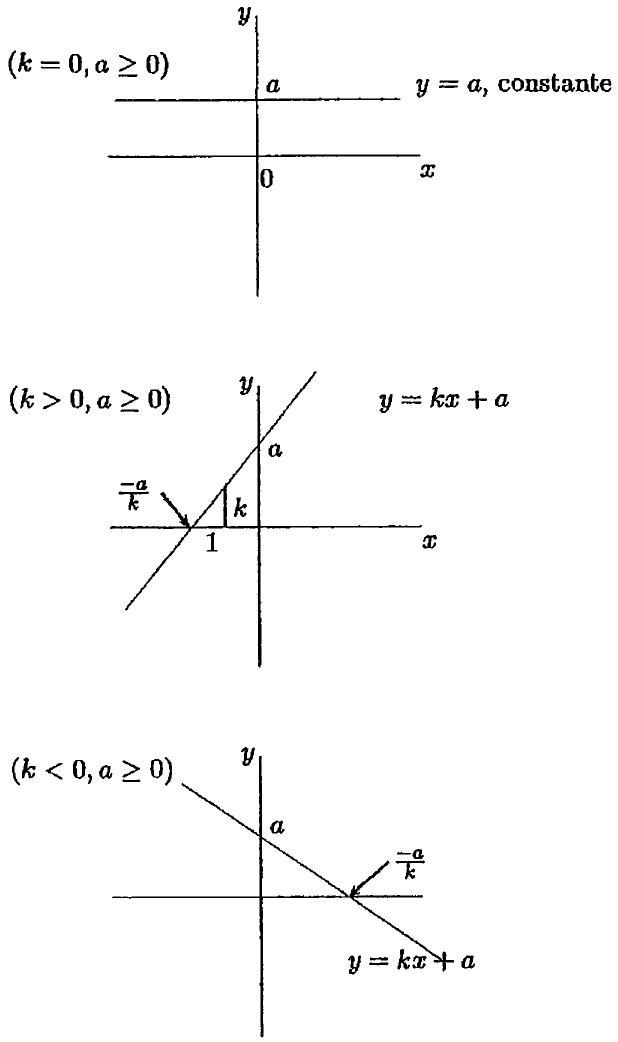


$y = kx$, homotecia por k

El diagrama representa el caso $k > 0$. Un movimiento Δx en las abscisas da lugar a un movimiento *multiplicado* $\Delta y = k\Delta x$ en las ordenadas: si $k > 1$ el movimiento aumenta (y la gráfica de la homotecia queda *por encima* de la diagonal), si $k < 1$ el movimiento disminuye (y la gráfica de la homotecia queda *por debajo* de la diagonal). Para el caso $k < 0$ se tendrá una *inversión* de las diagonales. Para el caso $k = 0$ se tendrá una recta *paralela* al eje de las abscisas (ver el próximo caso).

A.4. Lineal general: $f : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto kx + a$

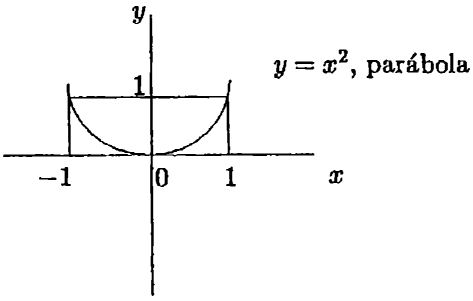
La función lineal general es la compuesta de una homotecia y una traslación: $f = t_{-a} \circ h_k$, pues $t_{-a} \circ h_k(x) = t_{-a}(h_k(x)) = t_{-a}(kx) = kx - (-a) = kx + a = f(x)$ (cuidado: la composición inversa da lugar a *otra* función lineal diferente de f). Como puede verse en los diagramas siguientes, las gráficas de las funciones lineales son *siempre líneas rectas*, ya sea diagonales (si $k \neq 0$), ya sea horizontales (si $k = 0$).



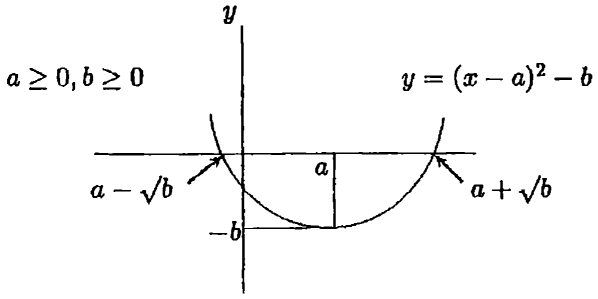
Los demás casos de gráficas de funciones lineales se obtienen de manera similar (ejercicio 11.1), mediante adecuados movimientos de las diagonales a lo largo del plano. Todos los casos de rectas en el plano representan así alguna función lineal, *excepto* los casos de rectas paralelas al eje de las ordenadas, que *no* pueden representar funciones (¿por qué?).

Pasamos ahora a observar las gráficas de funciones cuadráticas.

B.1. Parábola sencilla: $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2$

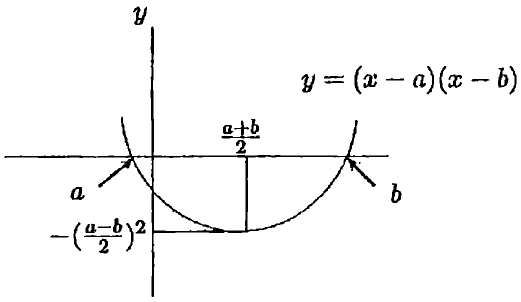


B.2. Traslaciones de parábolas: $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto (x-a)^2 - b$



La parábola anterior resulta de una *doble traslación*: con respecto a x (fragmento $(x-a)^2$) y con respecto a y (fragmento $-b$). En el caso diagramado ($a \geq 0, b \geq 0$), ésto corresponde a desplazar la parábola sencilla hacia la derecha (hasta llegar a $x = a$) y hacia abajo (hasta llegar a $y = -b$: éste es el mínimo valor de la nueva parábola, pues $(x-a)^2$ sólo agrega valores positivos a la función). Las *raíces* de la parábola están representadas por los puntos en los que la parábola *cruza* el eje de las abscisas. En el caso $b \geq 0$, ésto siempre se va a dar, pues $(x-a)^2 - b = 0$ puede resolverse en $\mathbb{R}$, mediante $(x-a)^2 = b$, es decir $x = a \pm \sqrt{b}$ (existe en $\mathbb{R}$ pues $b > 0$). Para el caso $b < 0$, la parábola se sitúa toda entera en el cuadrante superior estrictamente positivo ($y > 0$), la parábola no cruza el eje de las abscisas y no se tienen raíces (en $\mathbb{R}$).

B.3.Parábola con raíces prescritas: $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto (x-a)(x-b)$



Esta parábola resulta ser un caso particular de las traslaciones anteriores (caso B.2), como puede verse gracias a los cálculos $(x-a)(x-b) = x^2-(a+b)x+ab = (x-\frac{a+b}{2})^2-(\frac{a+b}{2})^2+ab = (x-\frac{a+b}{2})^2-(\frac{a-b}{2})^2$. La primera igualdad surge del desarrollo inmediato del producto, la segunda igualdad se deriva del *completamiento de un cuadrado*, la tercera igualdad es un cálculo algebraico elemental (hacerlo!). Aquí, el completamiento de un cuadrado es una herramienta básica:

$$x^2+bx+c = (x+\frac{b}{2})^2+c-(\frac{b}{2})^2 = (x+\frac{b}{2})^2+\frac{4c-b^2}{4}.$$

Si b^2-4c («discriminante») es positivo, entonces la ecuación $(x+\frac{b}{2})^2+\frac{4c-b^2}{4} = 0$, que equivale a $(x+\frac{b}{2})^2 = \frac{b^2-4c}{4}$, puede resolverse en $\mathbb{R}$, y su solución es

$$x = -\frac{b}{2} \pm \sqrt{\frac{b^2-4c}{4}} = \frac{1}{2}(-b \pm \sqrt{b^2-4c}).$$

B.4. Homotecias de parábolas: $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto kx^2$

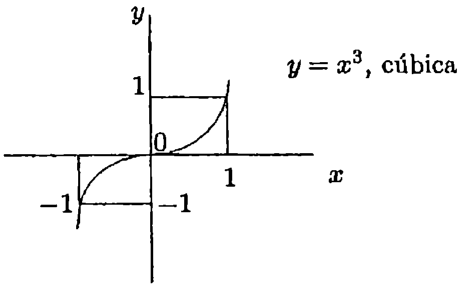
En el caso $k \geq 0$, las homotecias «alargan» o «aplastan» a la parábola sencilla $f(x) = x^2$. Si $k > 1$, la parábola inicial se alarga, y se aglutina sobre el eje de las ordenadas (ejercicio 11.2). La pendiente de la parábola en el punto $x = 1$ es igual a $2k$: crece a medida que k crece. En cambio, si $0 < k < 1$, la parábola inicial se aplasta, y se aglutina sobre el eje de las abscisas; la pendiente en $x = 1$ decrece a medida que k se acerca a 0. Si $k = 0$, la parábola se aplasta completamente y se convierte en el eje de las abscisas.

En el caso $k < 0$, las homotecias *invierten* a la parábola inicial $f(x) = x^2$ (ejercicio 11.2). Mediante combinaciones de traslaciones y homotecias

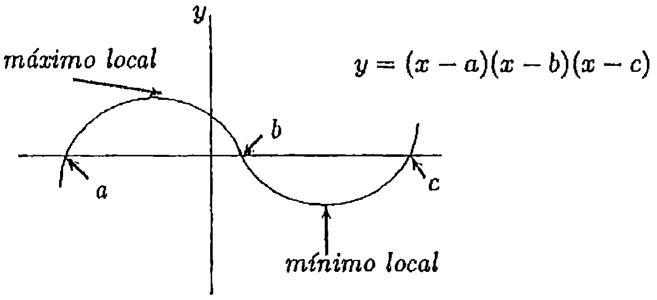
de parábolas, se pueden describir entonces todas las gráficas de funciones cuadráticas. Para un manejo adecuado de estas cuestiones, el estudiante deberá realizar unos cuantos cálculos y gráficas en casos particulares (ejercicio 11.3).

Señalamos brevemente a continuación el comportamiento general de las funciones cúbicas.

C.1. Cúbica sencilla: $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^3$



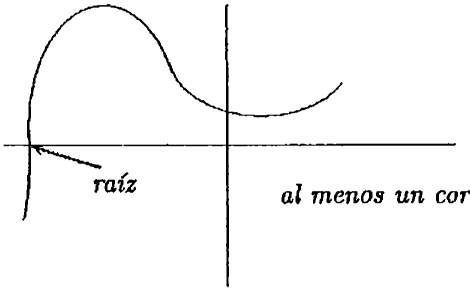
C.2. Cúbica con raíces prescritas: $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto (x-a)(x-b)(x-c)$



En la figura anterior, el máximo y el mínimo son *locales*, es decir, el valor en el máximo es mayor que los valores de la función en *vecindades pequeñas adecuadas* alrededor de ese máximo, y el valor en el mínimo es menor que los valores de la función en *vecindades pequeñas adecuadas* alrededor del mínimo. No podremos encontrar máximos o mínimos *absolutos*, puesto que

estas funciones se acercan al infinito cuando los valores de la variable se acercan al infinito. De hecho, intercambiando si es necesario signos en el infinito, *todas* las funciones que hemos revisado en esta sección tienen un comportamiento «similar» en el infinito. En la próxima sección, señalaremos el significado profundo que se encuentra detrás de estos comportamientos «similares».

C.3. Cúbica general: $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^3 + bx^2 + cx + d$



al menos un corte con el eje $y = 0$

El axioma fundamental de continuidad (o de completitud, véase la sección 9.4) es el que permite asegurar la existencia del *corte* entre la gráfica de la función cúbica y el eje de las abscisas. En muchos casos, el cálculo *explícito* de ese corte (raíz de la función cúbica) puede ser extremadamente difícil de encontrar en la práctica. Para ello, serán importantes los métodos que el estudiante descubra, por ejemplo, en un curso de ANÁLISIS NUMÉRICO. Por otro lado, en un curso posterior de ANÁLISIS, el estudiante revisará con detenimiento el fondo teórico detrás de esos procesos de corte, ligados a teoremas fundamentales de las funciones de variable real («teorema de Bolzano-Weierstrass[1]», «teorema de los valores intermedios»).

---

[1] Bernhard Bolzano (Bohemia, 1781-1848) fue el gran precursor del rigor matemático en el manejo de las colecciones infinitas. Karl Weierstrass (Alemania, 1815-1897) fue uno de los sistematizadores del análisis matemático a fines del siglo XIX. Su programa de *aritmetización del análisis* logró reducir muchos difusos conceptos analíticos a bases aritméticas más sólidas.

Desde un punto de vista global, *sintético*, o *relacional general*, las gráficas de las funciones de variable real tienen buenas propiedades geométricas que permiten reflejar ciertas propiedades analíticas subyacentes.

Definición 11.1. Sea f una función de $\mathbb{R}$ en $\mathbb{R}$.

f es **par** si y sólo si $\forall x \in \mathbb{R}\ f(-x) = f(x)$

f es **impar** si y sólo si $\forall x \in \mathbb{R}\ f(-x) = -f(x)$.

Por ejemplo, el estudiante revisará que la función cuadrática sencilla (B.1) es par, y que la función identidad (A.1) y la función cúbica sencilla (C.1) son impares. La *paridad* de la función se expresa geométricamente observando que la gráfica de la función es *simétrica con respecto al eje de las ordenadas*. La *imparidad* se expresa geométricamente observando que la gráfica es *simétrica con respecto al origen*, intersección de los ejes de coordenadas. Para otros ejemplos y generalizaciones de estas situaciones, véanse los ejercicios 11.5 y 11.6.

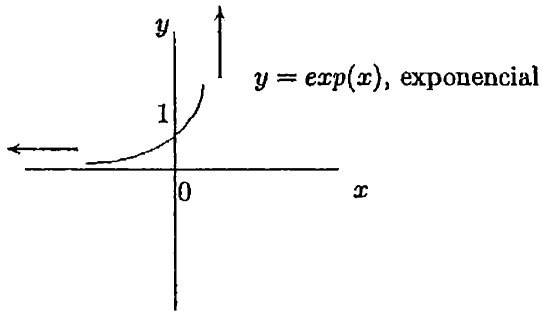
Por otro lado, es inmediato verificar que una función es *inyectiva* si y sólo si su gráfica corta todas las rectas horizontales ($y = b$) *a lo sumo* una vez (puede no cortarlas, pero no puede cortarlas dos veces). Igualmente, una función es sobreyectiva si y sólo si su gráfica corta todas las rectas horizontales *al menos* una vez (puede cortarlas más veces, pero no puede dejar de cortarlas). Para ejemplos, véase el ejercicio 11.7.

Para entender el comportamiento de un conjunto es útil salirse del conjunto y considerar sus transformaciones externas. En el caso del conjunto de los números reales, es útil considerar las funciones de $\mathbb{R}$ en $\mathbb{R}$ (o, más generalmente, las funciones de $\mathbb{R}$ en X para conjuntos adecuados X), y poder entonces operar sobre ellas. Los objetos de estudio *no son ya entonces elementos* de $\mathbb{R}$, sino funciones $\mathbb{R} \longrightarrow \mathbb{R}$. El estudio general de este *cambio de perspectiva* se realizará en cursos posteriores de la Carrera de Matemáticas, como ANÁLISIS FUNCIONAL, MEDIDA O TEORÍA DE REPRESENTACIONES. Sin embargo, es fácil ver aquí cómo pueden *sumarse y multiplicarse* funciones de $\mathbb{R}$ en $\mathbb{R}$: si f y g son funciones $\mathbb{R} \longrightarrow \mathbb{R}$, *definimos* $f+g$ y $f \cdot g$ (funciones de $\mathbb{R}$ en $\mathbb{R}$) mediante las reglas

$$(f+g)(x) = f(x) + g(x)\ ,\ (f \cdot g)(x) = f(x) \cdot g(x).$$

No debe confundirse aquí la multiplicación de funciones con su composición. Por ejemplo, si $f : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2$, y $g : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^3$, tenemos que $(f \cdot g)(x) = f(x) \cdot g(x) = x^2 \cdot x^3 = x^5$, mientras que $(f \circ g)(x) = f(g(x)) = f(x^3) = (x^3)^2 = x^6$. Para otros ejemplos, véase el ejercicio 11.9.

Una función imprescindible en matemáticas, de enorme poder técnico y conceptual, es la **función exponencial** $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto exp(x)$, cuya gráfica se presenta en la figura siguiente:



Para mayor sencillez, se denota a menudo $e^x = exp(x)$. En particular, se denota $e = e^1 = exp(1)$. La exponencial es una función que verifica las reglas

$$exp(0) = 1 \ , \ exp(x)exp(y) = exp(x + y).$$

Así, la exponencial transforma sumas en multiplicaciones, y se «ancla» en la condición inicial $exp(0) = 1$. Puede decirse, tal vez, que la función exponencial es la «función reina» en matemáticas; veremos destellos de la riqueza de esta función en la sección siguiente y en los capítulos 13 y 14, pero el lugar natural para asombrarse acerca de la profunda multiformidad de la exponencial será un curso posterior de VARIABLE COMPLEJA.

En el caso en que una función $f : \mathbb{R} \longrightarrow \mathbb{R}$ es inyectiva, la inversa f^{-1} (que siempre existe como relación) puede definirse *como función* desde el codominio de f. En efecto, $f^{-1} : cod(f) \longrightarrow \mathbb{R} : f(x) \mapsto x$ está bien definida (con imágenes únicas) gracias a que f es 1-1. La exponencial es 1-1 sobre su codominio, $cod(exp) = \mathbb{R}^+$. Por tanto, existe la *inversa* de la exponencial. La inversa resulta ser una función de $\mathbb{R}^+$ en $\mathbb{R}$, que llamamos **logaritmo**: $ln : \mathbb{R}^+ \longrightarrow \mathbb{R} : exp(x) \mapsto x$ (la notación ln se debe a razones históricas, para designar el «logaritmo neperiano», en homenaje a su inventor Neper[2]). Esta definición puede escribirse mediante la equivalencia $y = exp(x) \leftrightarrow ln(y) = x$,

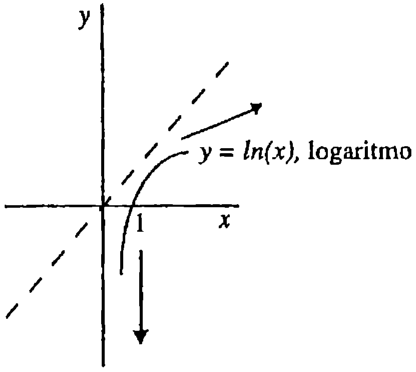
---

[2] John Neper (Escocia, 1550-1617) sirve como ejemplo del inventor matemático que elabora un concepto totalmente abstracto (en este caso, los logaritmos) para simplificar cálculos muy reales. El uso de los logaritmos en la astronomía y en la física del Renacimiento y la Ilustración ayudó de manera considerable al avance de las ciencias prácticas.

de donde se deducen las propiedades fundamentales del logaritmo (ejercicio 11.10):

$$ln(1) = 0\ ,\ ln(xy) = ln(x) + ln(y).$$

Así, el logaritmo transforma multiplicaciones en sumas. El interés de estas transformaciones fue muy grande en un momento en el que no se contaba con las poderosas máquinas de cálculo actuales, pues sirvió para reducir cálculos complicados a otros más elementales (es el caso también de las congruencias: ver final de la sección 8.2). La gráfica del logaritmo se obtiene mediante una simetría de la función exponencial *con respecto a la diagonal* $y = x$:



El caso de las gráficas del logaritmo y la exponencial es un caso particular de una situación mucho más general. De hecho, si f es una función *inyectiva* de $\mathbb{R}$ en $\mathbb{R}$ cuya gráfica denotamos $graf(f)$, entonces f^{-1} es una función de $cod(f)$ en $\mathbb{R}$, cuya gráfica $graf(f^{-1})$ se obtiene a partir de $graf(f)$ *por simetría con respecto a la diagonal* $y = x$. En efecto, dos puntos (a, b), (c, d) en el plano $\mathbb{R} \times \mathbb{R}$ son simétricos con respecto a la diagonal si y sólo si $(c, d) = (b, a)$, y resulta claro, por la definición de inversa, que $(a, b) \in graf(f)$ si y sólo si $(b, a) \in graf(f^{-1})$.

11.2. Algebraicidad y trascendencia

Dentro del conjunto de los números reales, existen espacios vedados a las aproximaciones constructivas usuales. Más allá de los enteros y de los racionales, se abre el espacio de lo *no* racional. Pero en esa primera incursión hacia el exterior de lo racional, existen aún herramientas de control: muchos

números irracionales son raíces de ecuaciones sencillas (como $\sqrt{2}$, raíz de $x^2 - 2 = 0$). Yendo más allá, en una segunda incursión hacia las *fronteras del no*, aparecen ciertos números que no son siquiera describibles como raíces de ecuaciones: los números «trascendentes». Nos ocupamos en esta sección de la definición de esos números que *trascienden* todo control ecuacional. La situación es sorprendente: hay tantos núneros trascendentes como hay reales, y nos encontramos entonces ante una verdadera *explosión* que, una vez más, va en contra de nuestra intuición (finitaria, natural o racional). Se trata de una coyuntura similar a la que emerge en los teoremas de Cantor (4.14, 4.15) o en el crecimiento descontrolado del universo de conjuntos (10.2).

Definición 11.2. Sea $a \in \mathbb{R}$. a se llama **algebraico** (sobre $\mathbb{Q}$) si y sólo si existen elementos $c_0, c_1, \ldots, c_n \in \mathbb{Q}$, no todos nulos, tales que $c_n a^n + c_{n-1}a^{n-1} + \cdots + c_2 a^2 + c_1 a + c_0 = 0$. a se llama **trascendente** en caso contrario.

Es fácil ver (¿por qué?) que un real es algebraico sobre $\mathbb{Q}$ si y sólo si es algebraico sobre $\mathbb{Z}$ (coeficientes $c_0, c_1, \ldots, c_n \in \mathbb{Z}$). Por tanto, cuando resulte más cómodo, bastará con considerar coeficientes enteros, en vez de racionales. Obsérvese que, en principio, puede llegar a ser muy difícil mostrar que un número es trascendente: la trascendencia obliga a demostrar que *no existe ninguna* combinación posible $c_n a^n + c_{n-1}a^{n-1} + \cdots + c_2 a^2 + c_1 a + c_0$ que sea igual a 0. En principio, habría que recorrer todas esas combinaciones: como son infinitas (¿por qué?) el problema es delicado. Las pruebas por contradicción no son nada evidentes tampoco en este contexto, y el matemático se aboca a problemas realmente arduos[3].

Ejemplo 11.3. (i). Todo racional es algebraico. Si $a \in \mathbb{Q}$, tome $c_0 = -a \in \mathbb{Q}$: se tiene $c_0 + a = 0$.

(ii). Cuando existe, toda raíz n-ésima de un racional es un número algebraico. Sea $\sqrt[n]{b}$ con $b \in \mathbb{Q}$, de tal manera que la raíz exista (en $\mathbb{R}$). Tome $c_0 = -b$, $c_n = 1$, $c_j = 0$ si $0 < j < n$ (todos los c_j son entonces racionales): se tiene entonces que $c_n(\sqrt[n]{b})^n + c_0 = b - b = 0$.

---

[3] Alan Baker (Inglaterra, n. 1939) y Michel Waldschmidt (Francia, n. 1946) son dos de los pocos matemáticos del siglo XX en haber obtenido algunos avances estructurales en la comprensión de los números trascendentes. Es un campo de investigación aún tremendamente desconocido.

(iii). e y π (longitud de un semicírculo de radio 1) son trascendentes. Se trata de dos difíciles resultados (debidos, respectivamente, a Hermite y Lindemann[4]), que abrieron la caja de Pandora de la trascendencia. En algún buen curso de ANÁLISIS o de SUCESIONES Y SERIES *tal vez* tenga el estudiante la oportunidad de acercarse a estas pruebas.

Más adelante, en cursos avanzados de CÁLCULO, se demostrará que la función exponencial puede escribirse como una *suma infinita* de funciones:

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} + \cdots$$

Observando que $1 + \frac{x}{1!} = 1 + x$ es lineal, que $1 + \frac{x}{1!} + \frac{x^2}{2!} = 1 + x + \frac{x^2}{2}$ es cuadrática, que $1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6}$ es cúbica, y así sucesivamente, vemos que la función exponencial *trasciende todas las aproximaciones finitarias* del tipo $1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$. En el próximo capítulo, llamaremos *polinomios* a este tipo de aproximaciones finitarias: por tanto, *la exponencial trasciende a todos los polinomios.* Nos encontramos aquí ante la emergencia de un paradigma muy fuerte en los conjuntos de números, según el cual se contrastarán argumentos *constructivos* (ligados a racionales, polinomios y funciones de aproximación) con argumentos *existenciales* (ligados a trascendencia e infinitudes altas). En buena medida, muchas de las técnicas más fructíferas en matemáticas intentarán cubrir esa *brecha* entre lo efectivamente *construible* y lo meramente *existente.*

En los ejercicios 6.5 y 6.6 prefigurábamos el hecho de que el conjunto de los números algebraicos Alg es enumerable. Si denotamos con $Trasc$ al conjunto de los números trascendentes, se tiene que $\mathbb{R} = Alg \cup Trasc$ (definición 11.2), y como $\mathbb{R}$ no es enumerable (teorema de Cantor), $Trasc$ no puede entonces ser enumerable (¿por qué?). Más aún, en esta situación se deduce obligatoriamente que $Trasc \sim \mathbb{R}$ (ejercicios 6.7 y 11.12). El ámbito

---

4 Charles Hermite (1822-1901) demostró la trascendencia de e en 1873. Ferdinand von Lindemann (Alemania, 1852-1939) demostró la trascendencia de π en 1882. Hermite repetía la famosa frase de Kronecker: «Dios ha creado los naturales y el resto es obra del hombre», y añadía, como un constructivista convencido: «Me giro con horror ante la lamentable plaga de funciones continuas sin derivadas».

de la trascendencia es entonces *inconmensurablemente más amplio* que el de la algebraicidad (si el estudiante incorpora aquí las enseñanzas de la sección 10.2, el término «inconmensurable» adquiere aquí toda su fuerza!). Es una situación paradójica puesto que lo poco que conocemos tiende a dirigirse, no obstante, hacia lo algebraico.

Ante este bloqueo, sorprende una vez más que la matemática consiga explorar los *bordes* de lo construible (finitario o algebraico), y no deje de ampliar su espectro hacia direcciones insospechadas, tratando de *trascender* las limitantes de *todo* subcampo de la disciplina. La *dialéctica pendular* entre álgebra y topología, entre finitud e infinitud, entre lógica y geometría, ha sido fuente de asombrosa creatividad desde mediados del siglo XIX hasta hoy. En medio de esas tirantes dialécticas, la matemática se encuentra a comienzos del siglo XXI en un espectacular *estado de gracia*, tremendamente viva, siempre sorprendente, cada vez más inventiva.

11.3. Ejercicios

11.1. Realice las gráficas de las demás funciones lineales que no se presentaron en el cuerpo del texto. Haga las gráficas en algunos casos particulares, así como en los casos generales no contemplados ($k < 0$, $a \leq 0$, etc.).

11.2. Realice las gráficas de homotecias de parábolas: $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto kx^2$. Contemple los casos $k > 1$, $k = 1$, $0 < k < 1$, $k = 0$, $-1 < k < 0$, $k = -1$, $k < -1$.

11.3. Realice las gráficas de las funciones cuadráticas siguientes:

(i) $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2 + x + 1$

(ii) $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2 + x - 2$

(iii) $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x^2 - x + 1$

(iv) $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto 3x^2 + 2x - 5$.

Realice otros ejemplos de gráficas de cuadráticas, tomando sus coeficientes como desee.

11.4. Sea $f : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto [x] = max\{y \in \mathbb{Z} : y \leq x\}$ (parte entera de x). Realice la gráfica de f. Explique gráficamente por qué f no es sobre y por qué f no es 1-1.

11.5. Muestre que las homotecias (A.3) son impares. ¿Qué puede decir de las traslaciones lineales (A.2) y de las traslaciones de parábolas (B.2): son impares, son pares? Distinga aquellos casos en los que se puede asegurar algo en general, de aquellos casos donde no vale ni paridad, ni imparidad.

11.6. Sean $a \in \mathbb{R}$, $f : \mathbb{R} \longrightarrow \mathbb{R}$. Decimos que f es par con respecto a a si y sólo si $\forall x \in \mathbb{R}\ f(-x+a) = f(x+a)$, y que f es impar con respecto a a si y sólo si $\forall x \in \mathbb{R}\ f(-x+a) = -f(x+a)$. Explique geométricamente qué significa paridad con respecto a a, e imparidad con respecto a a. Muestre que toda traslación $t_a : \mathbb{R} \longrightarrow \mathbb{R} : x \mapsto x - a$ es impar con respecto a a. Muestre que toda traslación de parábolas $\mathbb{R} \longrightarrow \mathbb{R} : x \mapsto (x-a)^2$ es par con respecto a a. Compare esta situación con el ejercicio 11.5.

11.7. Muestre *geométricamente* (es decir, explorando el comportamiento de una gráfica con respecto a *todas* las rectas horizontales) que la función identidad (A.1), las traslaciones (A.2), las homotecias no nulas (A.3) y la función cúbica sencilla (C.1) son inyectivas y sobreyectivas. Con el mismo tipo de argumentos *geométricos*, muestre que la función cuadrática sencilla (B.1), las traslaciones de parábolas (B.2) y algunas funciones cúbicas (dar dos ejemplos particulares) no son inyectivas. Explique *geométricamente*, en cambio, por qué toda función cúbica es sobreyectiva.

11.8. Diga si las siguientes frases son verdaderas o falsas, y explique las razones de su respuesta. En todo el ejercicio se trabaja con funciones de $\mathbb{R}$ en $\mathbb{R}$.

(i) La gráfica de f^{-1} (cuando existe) es simétrica a la gráfica de f con respecto al eje de las ordenadas.

(ii) La gráfica de la inversa de una función constante es una diagonal.

(iii) La gráfica de la inversa de una parábola es una parábola.

(iv) La gráfica de la inversa de una función par no corresponde a la gráfica de una función.

11.9. Demuestre que toda función $f : \mathbb{R} \longrightarrow \mathbb{R}$ puede expresarse (de manera única) como la suma de una función par y una función impar.

11.10. Complete la tabla siguiente, donde f y g son funciones de $\mathbb{R}$ en $\mathbb{R}$:

f	g	$f+g$	$f \cdot g$	$f \circ g$
$r \mapsto \sqrt{\lvert r \rvert}$	$r \mapsto r^2$			
$r \mapsto r + \sqrt{2}$	$r \mapsto 0$			
$r \mapsto 1 + r$	$r \mapsto r^{-1} (r \neq 0); 0 \mapsto 0$			

11.11. Partiendo de las propiedades de la función exponencial y de la definición de logaritmo como *inversa* de la exponencial, demuestre las propiedades de la función logaritmo indicadas en el texto.

11.12. Muestre que $Trasc \sim \mathbb{R}$ (donde $Trasc$ es el conjunto de los números trascendentes). De forma más general, muestre que si tenemos $X = Y \cup Z$, $Y \sim \mathbb{N}$ y $X \nsim \mathbb{N}$ entonces $Z \sim X$. Estamos expresando aquí, con mayor amplitud matemática y con mejor precisión formal, el ejercicio 6.7.

Capítulo 12

Polinomios y fracciones racionales

Contenido

12.1. Polinomios 128
12.2. Irreducibilidad 136
12.3. Fracciones racionales 138
12.4. Ejercicios 140

En este capítulo introducimos los polinomios, que merecen verse como los *objetos privilegiados* para el control *algebraico* de las extensiones de conjuntos de números. Los polinomios incorporan dos ideas fundamentales: *extender* un conjunto *allende una barrera operacional* dada, y hacerlo con una herramienta básicamente *finitaria*. Luego, con los cocientes de polinomios, es decir, con las fracciones racionales, se cierra la «transgresión» de la barrera.

12.1. Polinomios

Definición 12.1. Sea A un conjunto de números (en la práctica, A será igual a $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$: números complejos a definirse en el próximo capítulo). Un polinomio $P(X)$ con coeficientes en A es una expresión formal del tipo

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0$$

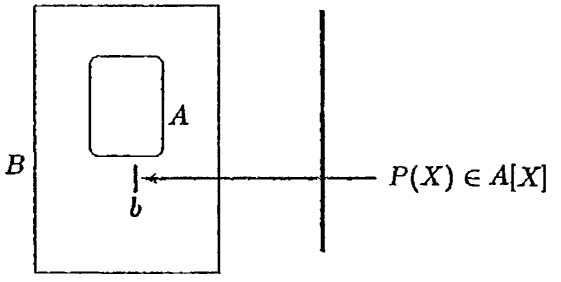
donde $a_n, a_{n-1}, \ldots, a_2, a_1, a_0$ son elementos de A.

El **conjunto de polinomios con coeficientes en** A se denota $A[X]$, es decir, $A[X] = \{a_n X^n + \cdots + a_0 : a_n, \ldots, a_0 \in A\}$. Trabajaremos aquí con una sola «variable» X (también llamada «indeterminada»), aunque en otras instancias (cursos de TEORÍA DE NÚMEROS o de ÁLGEBRA CONMUTATIVA) los polinomios en dos o más variables son de extrema importancia. Para mayor comodidad, escribiremos a menudo P para denotar al polinomio $P(X)$ (sobreentendiendo su variable X).

El **polinomio nulo** (denotado también 0) es aquel cuyos coeficientes son todos iguales a 0. El **grado** de un polinomio no nulo P (denotado por $grad(P)$) es el índice de su máximo coeficiente no nulo (llamado **coeficiente dominante**). El grado del polinomio 0 se define como $grad(0) = -\infty$. Un **monomio** es un polinomio del tipo $a_i X^i$, tal que todos sus coeficientes, excepto uno, son nulos.

Ejemplo 12.2. $X^2 + 1 \in \mathbb{Z}[X]$ (grado 2). $X^3 - \frac{3}{2}X + 1 \in \mathbb{Q}[X]$, y *no* pertenece a $\mathbb{Z}[X]$ (grado 3). $X - \sqrt{2} \in \mathbb{R}[X]$, y *no* pertenece a $\mathbb{Q}[X]$ (grado 1).

Sean A y B dos conjuntos de números, con $A \subseteq B$. Si B es adecuadamente «cerrado» con respecto a suma y multiplicación, B se llama una **extensión** de A: esto sucede para los casos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ que consideraremos en este curso. Sea $b \in B - A$ un elemento cualquiera. Para intentar medir qué tan «alejado algebraicamente» se encuentra b de A (ver figura), los polinomios en $A[X]$ constituyen una herramienta muy poderosa.



conjuntos de números *objetos formales externos*

La «distancia algebraica» de b a A puede ser controlada mediante los polinomios $P(X) \in A[X]$. No deben aquí confundirse los objetos que entran en juego: por un lado, tenemos conjuntos de números, con contenencias *internas*

entre ellos; por el otro lado, tenemos objetos puramente formales, *externos*, que se *refieren* a esos conjuntos de números y a eventuales pertenencias (o no) de elementos a esos conjuntos.

Inversamente, dado un conjunto de números A, ese conjunto podría extenderse gracias a ciertos «testigos privilegiados» (raíces) ligados a ciertos polinomios en $A[X]$. En el capítulo siguiente, mostraremos por ejemplo cómo los números complejos se construyen a partir de los números reales *gracias* al polinomio X^2+1 y a sus raíces.

Definición 12.3. Sea $P(X)$ un polinomio en $A[X]$. Sea b un número en alguna extensión B de A (incluyendo el caso $B=A$). Decimos que b es una **raíz** de $P(X)$ si y sólo si $P(b)=0$.

Un caso paradigmático de *control* en ciertos conjuntos de números se tiene al considerar los números algebraicos reales Alg (sección 11.2). En efecto, los algebraicos son las raíces de los polinomios con coeficientes en $\mathbb{Q}$:

$$Alg = \{a \in \mathbb{R} : \exists P(X) \in \mathbb{Q}[X](P(X) \neq 0 \wedge P(a) = 0)\}.$$

Por otro lado, desde un punto de vista algebraico, los números trascendentes reales $Trasc$ son el ejemplo extremo del *descontrol*:

$$Trasc = \{a \in \mathbb{R} : \forall P(X) \in \mathbb{Q}[X](P(X) \neq 0 \rightarrow P(a) \neq 0)\}.$$

Los trascendentes están *más allá* de cualquier aproximación algebraica finitaria, y ningún polinomio los controla. Intuitivamente entonces, la «distancia algebraica» de los trascendentes a $\mathbb{Q}$ es *infinita*! (en cursos posteriores donde se estudie la TEORÍA DE GALOIS, el estudiante podrá darle un pleno sustento riguroso a esta intuición).

Las operaciones de **suma y multiplicación** entre polinomios se definen a continuación. Mediante esas operaciones, tendremos *suficientes representantes externos* para poder medir comportamientos de muy diversa índole entre los conjuntos de números que deseemos explorar. Sea A uno de los conjuntos de números $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, o $\mathbb{C}$.

Definición 12.4. Sean $P(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ y $Q(X) = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$ dos polinomios en $A[X]$. Supongamos, sin pérdida de generalidad, que $grad(P) = n \geq m = grad(Q)$. Definimos entonces:

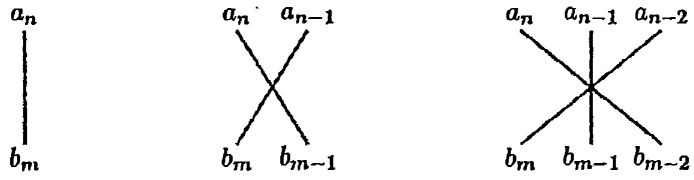
$$P(X)+Q(X)=$$

$$a_nX^n+a_{n-1}X^{n-1}+\cdots+(a_m+b_m)X^m+\cdots(a_1+b_1)X+(a_0+b_0)$$

$$P(X)Q(X)=$$

$$a_nb_mX^{n+m}+\cdots+\Big(\sum_{j+k=i}a_jb_k\Big)X^i+\cdots+(a_1b_0+a_0b_1)X+a_0b_0.$$

Así, la suma se realiza «componente por componente», sumando sencillamente los coeficientes de los polinomios. La multiplicación es más delicada: para cada monomio X^i su coeficiente se obtiene como un «producto cruzado»



a_nb_m $\qquad$ $a_nb_{m-1}+a_{n-1}b_m$ $\qquad$ $a_{n-2}b_m+a_{n-1}b_{m-1}+a_nb_{m-2}$

$\overbrace{\qquad}^{\text{coef } X^{n+m}}$ $\qquad$ $\overbrace{\qquad}^{\text{coef } X^{n+m-1}}$ $\qquad$ $\overbrace{\qquad}^{\text{coef } X^{n+m-2}}$

Este tipo de producto cruzado es un caso particular de una operación más general («convolución»), que el estudiante podrá explorar en cursos superiores (ÁLGEBRA LINEAL, ESTRUCTURAS ALGEBRAICAS, ANÁLISIS FUNCIONAL, ANÁLISIS ARMÓNICO) y que ayuda a codificar múltiples *trenzamientos* y *mixturas* que ocurren en las ciencias de la naturaleza.

Es inmediato verificar (hágalo!) que

$$grad(P+Q)\leq max(grad(P),grad(Q)).$$

El grado de una suma de polinomios no puede exceder el mayor de los grados, aunque el grado de la suma sí puede decrecer estrictamente. Esto sucede si y sólo si P y Q son de mismo grado y poseen coeficientes dominantes opuestos; por ejemplo, si $P(X)=X^2+X-1$ y $Q(X)=-X^2+3X-4$,

se tiene $P(X) + Q(X) = 4X - 5$, cuyo grado (igual a 1) es estrictamente menor al grado de P y al grado de Q (iguales a 2). Por otro lado, con los conjuntos de números que aquí consideramos, siempre se tiene que

$$grad(PQ) = grad(P) + grad(Q)$$

pues si $a_n(\neq 0)$ es el coeficiente dominante de P (es decir, P es de grado n) y $b_m(\neq 0)$ es el coeficiente dominante de Q (es decir, Q es de grado m), entonces el producto $a_n b_m$ no es nulo y es el coeficiente dominante de PQ (es decir, PQ es de grado $n+m$). Obsérvese que la ley fundamental que aquí se utiliza es la propiedad $a \neq 0 \wedge b \neq 0 \rightarrow ab \neq 0$. Se trata de una propiedad que es válida para los conjuntos de números aquí considerados ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$), pero que *podría no ser válida* en otro tipo de conjuntos de números. El estudiante descubrirá en cursos posteriores (ÁLGEBRA ABSTRACTA, ESTRUCTURAS ALGEBRAICAS) que existen muy interesantes conjuntos de números donde *no* vale esa propiedad, es decir, donde un producto de números no nulos puede ser nulo (para un adelanto, véase el ejercicio 12.4): en esos casos, el grado de un producto de polinomios podrá no ser igual a la suma de los grados de los polinomios.

Mediante la multiplicación de polinomios podrá expresarse, en cierta medida, la multiplicación de aquellos *entes ideales* que extiendan a los conjuntos de números. Los polinomios, con su multiplicación «convolutiva», son por tanto objetos algebraicos imprescindibles para el desarrollo de las matemáticas. Un *control* de esa multiplicación será entonces muy bienvenido. El algoritmo de división de Euclides, fundamento de la *operación* de multiplicación y de la *relación* de divisibilidad en $\mathbb{Z}$ (ver sección 8.2), se *extiende* a los conjuntos de polinomios $A[X]$ y provee el control deseado.

Algoritmo de división de Euclides para $A[X]$. Sean $P(X), Q(X) \in A[X]$, $Q \neq 0$ ($A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Existen entonces $S(X), R(X) \in A[X]$ (respectivamente, **cociente** y **resto** en la división) tales que

$$P(X) = Q(X)S(X) + R(X) \text{ con } grad(R) < grad(Q).$$

No demostraremos aquí el algoritmo de división. No obstante, lo asumiremos en este capítulo para obtener otros avances acerca de la estructura de los polinomios, y para manejar ciertos casos particulares. Puede darse que R sea igual a 0, y en ese caso se tiene automáticamente $grad(R) = -\infty < m = grad(Q)$, pues Q no es nulo y su grado es por tanto un natural. Cuando R es igual a 0, se tiene $P(X) = Q(X)S(X)$, y decimos que Q **divide** a P. La relación de divisibilidad en $A[X]$ es reflexiva y transitiva, pero no es ni simétrica, ni antisimétrica (ejercicio 12.3).

Ejemplo 12.5. Se solicita dividir el polinomio $P(X) = X^6 - X^4 - X^2 + 1$ por el polinomio $Q(X) = X^3 - 1$. El proceso de división es *recursivo*, y se lleva a cabo eliminando progresivamente las potencias *más altas*. En la figura siguiente se *dispone diagramáticamente* ese proceso recursivo:

$$
\begin{array}{llll|l}
X^6 & -X^4 & -X^2 & +1 & X^3 \quad -1 \\
\cline{5-5}
X^6 & & -X^3 & & X^3 \; -X \; +1 \\
\cline{1-3}
 & -X^4 & +X^3 & -X^2 \quad +1 & \\
 & -X^4 & & +X & \\
\cline{2-4}
 & & X^3 & -X^2 \; -X \; +1 & \\
 & & X^3 & \quad -1 & \\
\cline{3-4}
 & & & -X^2 \; -X \; +2 &
\end{array}
$$

El resultado de la división nos indica que hemos *obtenido* la igualdad $X^6 - X^4 - X^2 + 1 = (X^3 - 1)(X^3 - X + 1) + (-X^2 - X + 2)$. Puede *verificarse* esta igualdad desarrollando ahora el producto, con las convoluciones adecuadas. Sin embargo, una cosa es verificar una igualdad, y otra cosa muy distinta es obtenerla. El interés de un *algoritmo* como el de Euclides es que nos hace obtener la igualdad, y nos proporciona *explícitamente* un cálculo de los objetos en juego, algo que sólo de manera mucho más complicada podríamos realizar manejando sólo convoluciones. El cociente de la división es $X^3 - X + 1$ y el resto es $-X^2 - X + 2$; se verifica que el grado del resto (igual a 2) es estrictamente menor que el grado del polinomio por el cual se dividía (igual a 3).

Gracias al algoritmo de división de Euclides podemos ahora demostrar un resultado fundamental que entrelaza la problemática de extender campos de números mediante nuevos *números ideales*, con la problemática de la divisibilidad entre polinomios. En efecto, esos «números ideales» pueden construirse como *raíces* de ciertos polinomios, que resultan ser *múltiplos* de los polinomios lineales ligados a las raíces. Precisamos la situación en el siguiente teorema.

Teorema 12.6. *Sean $A \subseteq B$ dos conjuntos de números usuales (enteros, racionales, reales o complejos), sea $b \in B$, sea $P(X) \in A[X]$ (consúltese de nuevo el diagrama de la situación, presentado después del ejemplo 12.2). Entonces:*

$$b \text{ es raíz de } P(X) \quad \text{si y sólo si} \quad X - b \text{ divide } P(X) \text{ en } B[X].$$

Demostración. Si $X - b$ divide $P(X)$, entonces $P(X) = (X - b)Q(X)$, por tanto $P(b) = (b-b)Q(b) = 0Q(b) = 0$, es decir, b es raíz de P. La implicación inversa es la importante. Supongamos que b es raíz de P, es decir, $P(b) = 0$. Dividamos $P(X)$ por $X - b$ en $B[X]$ gracias al algoritmo de división de Euclides:

$$P(X) = (X - b)Q(X) + R(X), \text{ con } grad(R) < grad(X - b) = 1.$$

Se tiene entonces que $R = 0$ o $grad(R) = 0$, por tanto R es un polinomio constante: $R(X) = c$. Como $P(b) = 0$, se deduce $0 = P(b) = (b-b)Q(b)+c = 0Q(b) + c = 0 + c = c$, por tanto $c = 0$ y $P(x) = (X - b)Q(X)$, es decir, $X - b$ divide $P(X)$. Obsérvese que la prueba es muy sencilla *gracias al algoritmo de división*. Este algoritmo codifica toda la riqueza matemática de la prueba. □

Si *restringimos* A a los casos $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, los conjuntos de polinomios $A[X]$ poseen muy buenas propiedades de divisibilidad, parecidas a las de $\mathbb{Z}$. En particular, el máximo común divisor de dos polinomios se puede expresar también aquí como una «combinación lineal» de sus divisores. Para P, Q polinomios en $A[X]$, definimos $mcd(P, Q)$ como el polinomio máximo (para divisibilidad) que divide a P y Q, y cuyo coeficiente dominante es 1 (para evitar repeticiones del *mcd* mediante multiplicación por constantes). Se tiene entonces el siguiente **teorema de Bézout** para polinomios. Para los casos $A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$,

si $P, Q \in A[X]$, existen $R, S \in A[X]$ tales que $mcd(P, Q) = PR + QS$.

No demostraremos aquí este teorema (cuya prueba se pospone a cursos posteriores de ÁLGEBRA ABSTRACTA o de ESTRUCTURAS ALGEBRAICAS), pero un ejemplo es instructivo. Considérense, por ejemplo, $P(X) = 2X^4 + 2X^3 + 5X^2+3X+3$ y $Q(X) = X^3-1$. Realizando el algoritmo de Euclides repetidamente, obtenemos el $mcd(P, Q)$, y, devolviéndonos recursivamente mediante el algoritmo (véase el cálculo realizado antes de la definición 8.6), obtenemos R y S.

$$
\begin{array}{rrrrr|rr}
2X^4 & +2X^3 & +5X^2 & +3X & +3 & X^3 & -1 \\
\cline{6-7}
2X^4 & & & -2X & & 2X & +2 \\
\cline{1-5}
 & 2X^3 & +5X^2 & +5X & +3 & & \\
 & 2X^3 & & & -2 & & \\
\cline{2-5}
 & & 5X^2 & +5X & +5 & &
\end{array}
$$

Con esto, se obtiene entonces, en la división euclidiana, $P(X) = Q(X)(2X+2)+(5X^2+5X+5)$. Continuando con las divisiones (véase el ejemplo incluido antes de la definición 8.6), pasamos a dividir ahora $Q(X)$ por $5X^2+5X+5$:

$$
\begin{array}{rrrr|rrr}
X^3 & & & -1 & 5X^2 & +5X & +5 \\
\cline{5-7}
X^3 & +X^2 & +X & & \frac{1}{5}X & -\frac{1}{5} & \\
\cline{1-4}
 & -X^2 & -X & -1 & & & \\
 & -X^2 & -X & -1 & & & \\
\cline{2-4}
 & & & 0 & & &
\end{array}
$$

El último resto no nulo en este proceso proporciona un *candidato* para el máximo común divisor. El máximo común divisor es el adecuado múltiplo de ese candidato que posea *coeficiente dominante igual a 1*. Por tanto, $mcd(P,Q) = X^2 + X + 1$. Reescribiendo entonces la primera división se obtiene $5X^2+5X+5 = P(X) - (2X+2)Q(X)$, por lo tanto $X^2+X+1 = \frac{1}{5}P(X) - \frac{2X+2}{5}Q(X)$, de donde $R(X) = \frac{1}{5}$ y $S(X) = -\frac{2X+2}{5}$.

Obsérvese que este ejemplo muestra que, aunque P, Q y su $mcd(P,Q)$ pertenecen todos a $\mathbb{Z}[X]$, los factores en la combinación lineal se *salen* de $\mathbb{Z}[X]$ y pertenecen a $\mathbb{Q}[X]$. No hay por tanto esperanza de obtener un teo-

rema de Bézout para $\mathbb{Z}[X]$, y hay que restringir el conjunto A a alguno de los casos $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, como señalábamos al comienzo.

12.2. Irreducibilidad

Las buenas propiedades de divisibilidad en los conjuntos de polinomios permiten definir un *análogo fundamental de la noción de número primo* en $\mathbb{Z}$.

Definición 12.7. Sea $P(X) \in A[X]$ ($A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). $P(X)$ es **irreducible** (en $A[X]$) si y sólo si P no puede descomponerse en un producto de dos polinomios (en $A[X]$) de grado estrictamente menor: no existen $S, T \in A[X]$ tales que $P = ST$, $grad(S) < grad(P)$ y $grad(T) < grad(P)$.

Obsérvese que todo polinomio lineal (grado 1) es automáticamente irreducible. Sin embargo, para polinomios no lineales, debe tenerse mucho cuidado con la propiedad de irreducibilidad, pues se trata de una propiedad eminentemente *contextual*. La irreducibilidad depende del universo A sobre el que se toman los coeficientes de los polinomios, y es muy sensible a cualquier cambio en el conjunto A. De hecho, la noción misma de primalidad en $\mathbb{Z}$ (análoga de irreducibilidad en $\mathbb{Z}[X]$) es contextual: 5 es primo en $\mathbb{Z}$ pero no lo es en $\mathbb{Z}[i]$ (ver ejercicio 13.7).

Por ejemplo, el polinomio $X^2 - 2$ es irreducible en $\mathbb{Q}[X]$ (pues una factorización posible del tipo $X^2 - 2 = (X + a)(X + b)$ fuerza las ecuaciones $a + b = 0$ y $ab = -2$, cuyas soluciones $a = -b = \sqrt{2}$ *sacan* a los coeficientes fuera de $\mathbb{Q}$), aunque $X^2 - 2$ puede ser fácilmente reducido en $\mathbb{R}[X]$ (mediante la factorización $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$, con polinomios con coeficientes en $\mathbb{R}$). De forma similar, el polinomio $X^2 + 1$ es irreducible en $\mathbb{R}[X]$ (pues una factorización posible del tipo $X^2 + 1 = (X + a)(X + b)$ fuerza las ecuaciones $a + b = 0$ y $ab = 1$, cuyas soluciones $a = -b = i$ involucran un «número imaginario» que *saca* a los coeficientes fuera de $\mathbb{R}$), aunque $X^2 + 1$ puede ser fácilmente reducido en $\mathbb{C}[X]$ (mediante la factorización $X^2 + 1 = (X - i)(X + i)$, con polinomios con coeficientes en $\mathbb{C}$).

La irreducibilidad de un polinomio está estrechamente ligada a la existencia de sus posibles raíces, pero la irreducibilidad y la existencia de raíces *no son equivalentes* en general. Sí se tiene siempre la implicación:

$P(X)$ irreducible no lineal en $A[X]$ implica P no posee raíces en A.

En efecto, por contrarrecíproca, si P posee una raíz $a \in A$ entonces $X - a$ es un polinomio en $A[X]$ que divide a P en $A[X]$ (teorema 12.6 tomando

el caso $A = B$), por tanto $P(X) = (X - a)Q(X)$ es reducible en $A[X]$. La implicación contraria, en cambio, no es siempre verdadera: pueden existir polinomios sin raíces que, no obstante, son reducibles. Considere el polinomio $X^4 + 2X^2 + 1$ en $\mathbb{R}[X]$; como $X^4 + 2X^2 + 1 = (X^2 + 1)^2$, el polinomio no posee raíces en $\mathbb{R}$ (sus raíces serán $\pm i \in \mathbb{C}$), pero es claramente reducible: $X^4 + 2X^2 + 1 = (X^2 + 1)(X^2 + 1)$. Sin embargo, para los polinomios *de grado* ≤ 3 sí vale que P sin raíces implica P irreducible (ejercicio 12.5).

Por otro lado, aunque todo polinomio de grado 1 es irreducible, *en general* no todo polinomio irreducible es de grado 1 (considere por ejemplo $X^2 - 2$ en $\mathbb{Q}[X]$). Sin embargo, como veremos pronto, un hecho de tremenda importancia, y que resulta ser la *razón de ser* del conjunto de los complejos, es que en $\mathbb{C}[X]$ sí se tiene en cambio la equivalencia

P es de grado 1 si y sólo si P es irreducible.

Así, en el conjunto de los complejos, los polinomios irreducibles se trivializan. Como veremos, ganamos entonces en raíces (resolución de todas las ecuaciones), pero perdemos en divisibilidad (trivialización de los candidatos a primos): otro ejemplo más de la incesante pendularidad de las matemáticas.

Como lo hemos hecho a todo lo largo de este capítulo, al hacer referencia a $\mathbb{C}$, nos estamos adelantando a los dos capítulos finales; el estudiante puede manejar aquí por el momento una información rudimentaria sobre los complejos (intuiciones a partir de su experiencia en el colegio), y volver luego a *reentender* estos conceptos, una vez haya estudiado los capítulos finales.

Ejemplo 12.8. En la tabla siguiente, damos algunos ejemplos de cómo la irreducibilidad y la existencia de raíces varían muy sensiblemente *según el contexto* en el que nos situemos. Para las pruebas, véase el ejercicio 12.6.

	contexto polinomial				*contexto numérico*			
polinomio	$\mathbb{Z}[X]$	$\mathbb{Q}[X]$	$\mathbb{R}[X]$	$\mathbb{C}[X]$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
	irreducibilidad				*raíces*			
$X^2 + X + 1$	sí	sí	sí	no	no	no	no	sí
$2X - 3$	sí	sí	sí	sí	no	sí	sí	sí
$X^2 + 1$	sí	sí	sí	no	no	no	no	sí
$X^3 - 2$	sí	sí	no	no	no	no	sí	sí
$X^p + 1$ (p impar ≥ 3)	no	no	no	no	sí	sí	sí	sí
$X^4 + 2X^2 + 1$	no	no	no	no	no	no	no	sí

12.3. Fracciones racionales

Al ampliar el universo de los polinomios, e invertirlos multiplicativamente, se extiende el rango de acción de los objetos matemáticos. Con esos nuevos entes («fracciones racionales»), no sólo medimos ya ciertas transferencias u obstrucciones algebraicas, sino que abrimos el camino a futuras consideraciones analíticas y geométricas. Las fracciones racionales serán de gran uso, de hecho, en cursos de CÁLCULO INTEGRAL, así como en cursos donde se estudie la geometría de los conjuntos de soluciones de ciertas ecuaciones (TEORÍA DE NÚMEROS, GEOMETRÍA ALGEBRAICA).

Definición 12.9. Sea A un conjunto de números ($A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Una **fracción racional** con coeficientes en A es una expresión formal del tipo

$$\frac{P(X)}{Q(X)}$$

donde $P, Q \in A[X], Q \neq 0$. El **conjunto de fracciones racionales con coeficientes en** A se denota $A(X)$, es decir, $A(X) = \{\frac{P(X)}{Q(X)} : P, Q \in A[X]\}$ (paréntesis cuadrados para conjuntos de polinomios, paréntesis redondos para conjuntos de fracciones racionales).

Si recordamos que *analizar* significa *descomponer* (simplificar de alguna manera lo compuesto, y convertirlo en elemental), un *análisis* del conjunto de las fracciones racionales apuntaría a expresar ciertas fracciones racionales a partir de otras fracciones más simples. Dentro de este panorama, dada una fracción racional $\frac{P}{Q}$, una **descomposición en fracciones simples de** $\frac{P}{Q}$ se realizará gracias a las dos etapas siguientes:

(i) descomponer Q en producto de irreducibles: $Q(X) = \prod_{1 \leq i \leq k} (q_i(X))^{j_i}$

(ii) descomponer $\frac{P}{Q}$ en sumas «simples»:

$$\frac{P(X)}{Q(X)} = \sum_{1 \leq i \leq k} \sum_{0 < j \leq j_i} \frac{a_{ij}(X)}{(q_i(X))^j}$$

donde $grad(a_{ij}) < grad(q_i)$.

De nuevo, estamos intentando calcar aquí un proceso que se da en el conjunto de los enteros, completado con el conjunto de sus inversos racionales. Por ejemplo, el racional $\frac{3}{28}$ podría «descomponerse en fracciones simples» si pudiéramos escribirlo bajo la forma $\frac{3}{28} = \frac{3}{2^2 7} = \frac{a}{2} + \frac{b}{2^2} + \frac{c}{7}$, lo que equivaldría,

reduciendo al mismo denominador, a resolver en enteros $14a+7b+4c=3$. No es ésta una ecuación obvia de resolver en $\mathbb{Z}$, pero podríamos hacerlo gracias al teorema de Bézout. Lo mismo sucederá con la descomposición en fracciones simples para el caso de las fracciones racionales. Es imposible en este momento demostrar un teorema de descomposición en su forma general, pero procedemos a mostrar cómo se realiza una descomposición en un caso particular. Por supuesto, el estudiante sabe ya que, con ese caso particular, no demuestra nada en general, pero puede confiar en que más adelante en su Carrera se realice esa prueba general.

Ejemplo 12.10. Nos situamos en $\mathbb{Q}(X)$ y se solicita descomponer en fracciones simples la fracción racional $\frac{P(X)}{Q(X)} = \frac{1}{(X^2+1)(X+1)^2}$. Según la forma general de la descomposición, debemos tener

$$\frac{1}{(X^2+1)(X+1)^2} = \frac{cX+d}{X^2+1} + \frac{a}{X+1} + \frac{b}{(X+1)^2} \qquad (*)$$

Hay esencialmente dos métodos para encontrar los coeficientes a, b, c, d que estamos buscando: uno vía usos repetidos del teorema de Bézout para polinomios, otro vía sistemas de ecuaciones para los coeficientes. El primero es más sistemático, pero tal vez sea más delicado teóricamente; el segundo es más azaroso, pues pueden introducirse más errores en los cálculos, pero tal vez sea más sencillo en la práctica (éste es un ejemplo más de la *oscilación pendular* en matemáticas: no hay «caminos reales», y, si ganamos algo por un lado, algo perdemos por el otro!).

Primer camino. Observamos el denominador $Q(X) = (X^2+1)(X+1)^2$. Como X^2+1 y $X+1$ son irreducibles (en el conjunto de polinomios $\mathbb{Q}[X]$), su *mcd* es entonces igual a 1, y podemos buscar expresarlo como una combinación lineal de Bézout. Tenemos $X^2+1 = (X+1)^2 - 2X$, y $(X+1)^2 = -2X(-\frac{1}{2}X-1)+1$ (mediante la división de polinomios: hágala!), de donde $1 = (X+1)^2(-\frac{1}{2}X) + (X^2+1)(\frac{1}{2}X+1)$. De aquí se deduce entonces

$$\frac{1}{(X^2+1)(X+1)^2} = \frac{(X+1)^2(-\frac{1}{2}X) + (X^2+1)(\frac{1}{2}X+1)}{(X^2+1)(X+1)^2}$$

$$= \frac{-\frac{1}{2}X}{X^2+1} + \frac{\frac{1}{2}X+1}{(X+1)^2} = \frac{-\frac{1}{2}X}{X^2+1} + \frac{\frac{1}{2}(X+1)+\frac{1}{2}}{(X+1)^2}$$

$$= \frac{-\frac{1}{2}X}{X^2+1} + \frac{\frac{1}{2}}{(X+1)} + \frac{\frac{1}{2}}{(X+1)^2}.$$

Si se compara esta expresión con la expresión buscada (*), resulta que tendremos $c = -\frac{1}{2}$, $d = 0$ y $a = b = \frac{1}{2}$.

Segundo camino. Reducimos la expresión (*) al *mismo denominador* y comparamos coeficientes. Se debe tener entonces

$$(cX + d)(X + 1)^2 + (a(X + 1) + b)(X^2 + 1) = 1,$$

de donde, igualando los coeficientes de cada uno de los monomios X^3, X^2, X y 1, se obtienen las ecuaciones

$a + c = 0$ (coeficiente de X^3)

$2c + d + a + b = 0$ (coeficiente de X^2)

$2d + c + a = 0$ (coeficiente de X)

$d + a + b = 1$ (coeficiente de 1).

La resolución de estas ecuaciones (despejando y reemplazando sucesivamente adecuadas variables en las ecuaciones) da lugar también a la solución encontrada con el primer método: $c = -\frac{1}{2}$, $d = 0$ y $a = b = \frac{1}{2}$.

Si se comparan los dos métodos, se ve cómo el primer método es *estructuralmente más estable*: hay una guía para el proceso, y la guía puede ayudar a conservar un cierto orden en los cálculos. Sin embargo, esa «estructuralidad estable» requiere manejar la teoría de Bézout. Por otro lado, el segundo método no requiere ninguna teoría, pero es más inestable: el practicante de ese método podrá fácilmente olvidar algún coeficiente, o realizar mal alguna substitución en las ecuaciones, y todo se dañará!

12.4. Ejercicios

12.1. Sea A uno de los conjuntos de números usuales ($A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Considere el conjunto de las funciones de $\mathbb{N}$ en A que son iguales a 0 «en casi todas partes»: $A^{<\mathbb{N}} =_{def} \{f : \mathbb{N} \longrightarrow A : f$ es función y $\exists n_f \forall n \geq n_f \ f(n) = 0\}$. Demuestre que entonces $A^{<\mathbb{N}} \sim A[X]$. Ayuda: sea $f_n : \mathbb{N} \longrightarrow A$ definida por $f_n(m) = 1$ si $m = n$ y $f_n(m) = 0$ si no; muestre que la correspondencia $f_n \mapsto X^n$ puede extenderse a una biyección entre $A^{<\mathbb{N}}$ y $A[X]$, utilizando adecuadas sumas de funciones y multiplicaciones de funciones por elementos.

12.2. Encuentre polinomios explícitos P y Q en $\mathbb{Z}[X]$ tales que $P(\sqrt{2}+\sqrt{3}) = 0$ y $Q(\sqrt{2} + \sqrt{3} + \sqrt{5}) = 0$.

12.3. Muestre que la relación de divisibilidad en $A[X]$ ($A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) no es simétrica y no es antisimétrica.

12.4. Sea $\mathbb{Z}_4$ el conjunto $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ con las operaciones de suma y multiplicación definidas en las tablas siguientes:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Así, la suma $+_4$ y la multiplicación $\cdot_4$ se obtienen tomando los *restos en la división por 4* de la suma y el producto usuales en los enteros. Encuentre P y Q en $\mathbb{Z}_4[X]$ tales que $grad(PQ) < grad(P) + grad(Q)$ (compare esta situación con la discusión sobre grados dada en la sección 12.1). Muestre que $X^4 + 1$ no posee raíces en $\mathbb{Z}_4$ y, no obstante, es reducible en $\mathbb{Z}_4[X]$.

12.5. Sea A uno de los conjuntos de números usuales ($A = \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Muestre que, para todo polinomio no lineal $P(X) \in A[X]$ con $grad(P) \leq 3$, se tiene: P irreducible si y sólo si P no posee raíces en A.

12.6. Demuestre todas las propiedades de los polinomios incluidas en la tabla del ejemplo 12.8.

12.7. Encuentre el máximo común divisor $D(X)$ de $P(X) = X^4 + X^3 - 5X^2 + X - 6$ y $Q(X) = X^4 + X^3 + 3X^2 + X + 2$. Encuentre explícitamente R y S tales que $D = PR + QS$. ¿Cuál es el mínimo conjunto de polinomios en el que nos podemos situar para realizar estos cálculos?

12.8. Considere la fracción racional (en $\mathbb{Q}(X)$)

$$\frac{P(X)}{Q(X)} = \frac{1}{X^2(X-1)^3}.$$

Descomponga la fracción racional en fracciones simples, utilizando los *dos métodos distintos* indicados en el texto. Debe, por tanto, encontrar $a, b, c, d, e \in \mathbb{Q}$ tales que

$$\frac{P(X)}{Q(X)} = \frac{a}{X-1} + \frac{b}{(X-1)^2} + \frac{c}{(X-1)^3} + \frac{d}{X} + \frac{e}{X^2}.$$

Capítulo 13

Números complejos

Contenido

13.1. Números complejos 143
13.2. Representaciones geométricas 144
13.3. Exponencial compleja 147
13.4. Ejercicios 151

En este capítulo introducimos el conjunto de los *números* complejos, fundamentando así ciertas observaciones mencionadas en el texto en ocasiones anteriores (particularmente en el capítulo 12, alrededor de los polinomios). En el capítulo siguiente (y final) revisamos algunas propiedades de algunas *funciones* sobre esos números, pero no pasamos de consideraciones muy elementales. Más allá de las breves informaciones proporcionadas en estos capítulos finales, la *teoría de funciones de variable compleja* merece ser considerada como una de las más bellas teorías de la matemática (si nos atrevemos, podríamos calificarla tal vez como *la más* bella creación de toda la matemática). El estudiante podrá vislumbrar toda la *riqueza* (armonía, solidez estructural, profundidad, sorpresa, aplicabilidad, etc.) de las funciones de variable compleja en otros cursos superiores, como VARIABLE COMPLEJA, ANÁLISIS ARMÓNICO o SUPERFICIES DE RIEMANN.

13.1. Números complejos

Consideremos el polinomio $P(X) = X^2 + 1 \in \mathbb{Z}[X]$. Hemos visto que P no posee raíces en $\mathbb{R}$, pero podemos asumir la *existencia* de una raíz de P en una *extensión* de $\mathbb{R}$. Si llamamos i a una de las raíces de P, tenemos que i verifica $P(i) = i^2 + 1 = 0$, es decir

$$i^2 = -1.$$

i se llama unidad *imaginaria* y la ecuación anterior define su comportamiento multiplicativo. Es claro que si i es raíz de P, entonces $-i$ también es raíz de P, pues $(-i)^2 = (-1)^2(i)^2 = i^2 = -1$. Tenemos por tanto la factorización de P (ver teorema 12.6): $P(X) = (X - i)(X + i)$.

Definición 13.1. El conjunto $\mathbb{C}$ de los **números complejos** se define como el conjunto de combinaciones lineales de 1 e i con coeficientes reales: $\mathbb{C} =_{def} \{a + bi : a, b \in \mathbb{R}\}$. Las reglas de las operaciones de suma, multiplicación y división en $\mathbb{C}$ se obtienen como *extensiones* de las reglas pertinentes en $\mathbb{R}$, *combinadas* con la regla de multiplicación $i^2 = -1$:

$(a + ib) + (c + id) = (a + c) + i(b + d)$ (suma)

$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$ (multiplicación)

$\frac{1}{a+ib} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$ (para $a + ib \neq 0$) (división).

En efecto, la segunda ecuación puede tomarse como definición, u obtenerse al *desarrollar* $(a+ib)(c+id)$ y agrupar los términos convenientemente, usando leyes de distribución, conmutación y asociación extendidas, así como la «ley» $i^2 = -1$. La tercera ecuación puede también tomarse como definición, u obtenerse en forma similar, usando leyes extendidas de asociatividad, conmutatividad y distributividad, al multiplicar numerador y denominador por $a-ib$, y observar que $(a+ib)(a-ib) = a^2+b^2$. Asumiendo leyes extendidas de conmutatividad, podremos escribir los complejos en diversas formas: $a + ib = a + bi = bi + a$, etc. Ejemplos concretos de operaciones son los siguientes (el estudiante deberá realizar a su gusto otros cálculos similares): $(1 - i) + i\sqrt{2} = 1 + i(\sqrt{2} - 1)$; $(1 + i)(1 - 2i) = 1 - 2i + i - 2i^2 = 3 - i$; $\frac{1}{1+i} = \frac{1-i}{1^2+1^2} = \frac{1}{2} - \frac{i}{2}$.

Definición 13.2. Denotaremos usualmente con la letra z a un número complejo: $z = a + ib$. a se llama la **parte real** de z, b se llama la **parte imaginaria** de z (obsérvese que, por definición, las partes real e imaginaria de un complejo son *ambas* números reales: $a, b \in \mathbb{R}$). Denotaremos $a = Re(z)$

la parte real, y $b = Im(z)$ la parte imaginaria. Dado $z = a + ib \in \mathbb{C}$, el conjugado de z (denotado $\overline{z}$) se define por $\overline{z} = a - ib$ (misma parte real, parte imaginaria opuesta).

El interés esencial de los conjugados consiste en poder *transferir* ciertos cálculos en $\mathbb{C}$ a cálculos en $\mathbb{R}$. Es inmediato, por ejemplo, que $z + \overline{z} = 2Re(z)$, eliminándose las partes imaginarias. Por otro lado, el producto de un complejo y de su conjugado es siempre también un número real: para todo $z \in \mathbb{C}$, $z\overline{z} = (a+ib)(a-ib) = a^2 + b^2 \in \mathbb{R}$. Si definimos (de la manera esperada) el número complejo 0 por $0 = 0 + i0$, la multiplicación por el conjugado nos muestra que $z\overline{z} = a^2 + b^2 = 0$ si y sólo si $a = b = 0$ si y sólo si $z = \overline{z} = 0$. Cuando $z \neq 0$, su inverso multiplicativo z^{-1} está dado entonces por $z^{-1} = \frac{1}{z} = \frac{\overline{z}}{z\overline{z}}$.

Con la construcción de los números complejos podemos resolver entonces la ecuación $X^2 + 1 = 0$. Un *hecho totalmente notable* es que, al resolver esta sencilla ecuación particular, y al añadir una raíz de la ecuación a los reales, podamos resolver entonces todas las (infinitas) ecuaciones posibles en $\mathbb{C}$ («teorema fundamental del álgebra»: sección 14.3). El paso de *una* raíz peculiar a *todas* las posibles raíces constituye una de las *transgresiones* más fuertes, en el paso de lo finito a lo infinito, realizadas en el curso de FUNDAMENTOS.

13.2. Representaciones geométricas

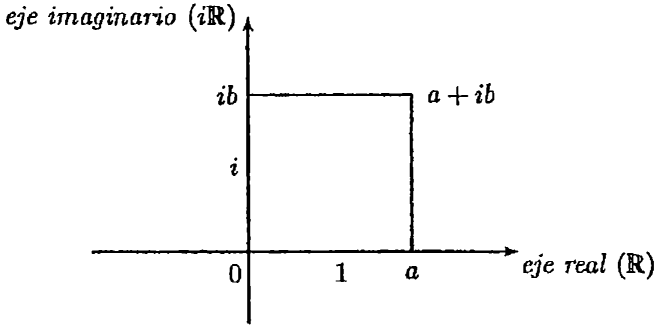
Los números complejos, introducidos en el siglo XVI para resolver de manera artificial («imaginaria») ciertas ecuaciones[1], adquirieron toda su fuerza en el

---

[1] Niccolò Fontana (Italia, 1500-1572), apodado *Tartaglia* (tartamudo), fue el primero en resolver las ecuaciones generales de tercer grado, introduciendo ciertas combinaciones «imaginarias» intermedias, que luego hacía desaparecer de los resultados finales. Gerolamo Cardano (Italia, 1501-1576) publicó y generalizó los resultados que le había comunicado Tartaglia. Al hacerlo sin el consentimiento de Tartaglia, surgió una fuerte disputa que se repetirá a menudo en las matemáticas posteriores: el inventor moderno querrá que la sociedad reconozca su prioridad!

siglo XIX gracias a un acertado manejo geométrico del concepto[2], y gracias a sus sorprendentes aplicaciones prácticas en la física matemática[3]. Presentamos a continuación las dos representaciones geométricas fundamentales de los números complejos.

Definición 13.3. Coordenadas cartesianas. Un número complejo $z = a + ib$ se representa en el plano cartesiano $\mathbb{R} \times \mathbb{R}$, mediante dos datos: su proyección (parte real) en el eje de las *abscisas*, y su proyección (parte imaginaria) en el eje de las *ordenadas*.



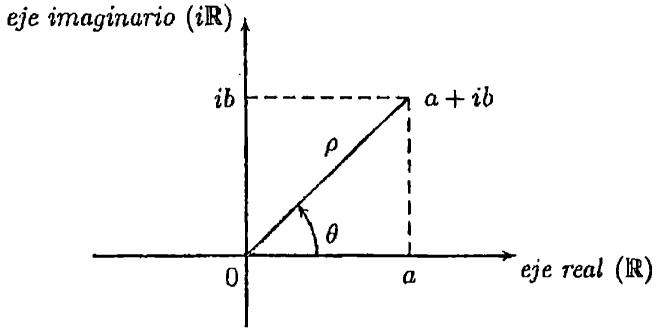
En esta representación, el *eje real* es el eje de las abscisas (igual al conjunto de los múltiplos reales de 1), y el *eje imaginario* es el eje de las ordenadas

2 Jean-Robert Argand (Francia, 1768-1822), un librero parisino aficionado a las matemáticas, introdujo de manera oficial (1806) la representación de los complejos sobre el plano $\mathbb{R} \times \mathbb{R}$. La representación ya era manejada por otros matemáticos en sus manuscritos (en particular, Gauss, ver sección 14.3), pero Argand fue el primero en publicar sus ideas.

3 Los trabajos de Cauchy y Riemann en funciones de variable compleja abren una compuerta espectacular a las aplicaciones. A fines del siglo XIX, la teoría del electromagnetismo se afianza gracias a la obra de James Clerk Maxwell (Escocia, 1831-1879). Maxwell establece las primeras leyes generales de la electricidad *gracias* al manejo de ecuaciones diferenciales con números complejos. De esta manera, todo nuestro mundo moderno, *dependiente* de la electricidad, se basa *irrevocablemente* en esa construcción imaginaria de los matemáticos inaugurada en el siglo XVI y que tomó cuatro siglos en encarnar!

(igual al conjunto de los múltiplos reales de i). El *conjugado* se obtiene aquí inmediatamente mediante una *simetría* con respecto al eje de las abscisas. La representación cartesiana es particularmente útil para graficar *sumas* de números complejos. En cambio, la *multiplicación* de complejos no se grafica de forma natural con estas coordenadas, y es útil contar con otra representación alternativa.

Definición 13.4. Coordenadas polares. Un número complejo z se representa en el plano mediante dos datos: su *distancia* ρ al origen, y su *ángulo* θ con el eje de las abscisas (escogiendo, por convención, ese ángulo entre 0 y 2π). La distancia ρ se llama el **módulo** de z (que denotamos por $|z|$); el ángulo θ se llama el **argumento** de z (que denotamos por $arg(z)$).



Las relaciones entre coordenadas cartesianas y coordenadas polares son fáciles de precisar. Supóngase primero que el complejo z está dado por sus coordenadas cartesianas: $z = a + ib$. Entonces, por el teorema de Pitágoras aplicado al triángulo cuyos vértices son 0, a y $a+ib$, se obtiene $\rho^2 = a^2 + b^2$, de donde

$$\rho = \sqrt{a^2 + b^2}.$$

Además, las definiciones de las funciones trigonométricas en el mismo triángulo nos proporcionan

$$\cos\theta = \frac{a}{\rho} \quad , \quad \sin\theta = \frac{b}{\rho}.$$

Supóngase ahora que el complejo z está dado por sus coordenadas polares ρ y θ. Entonces, sus coordenadas cartesianas se obtienen inmediatamente:

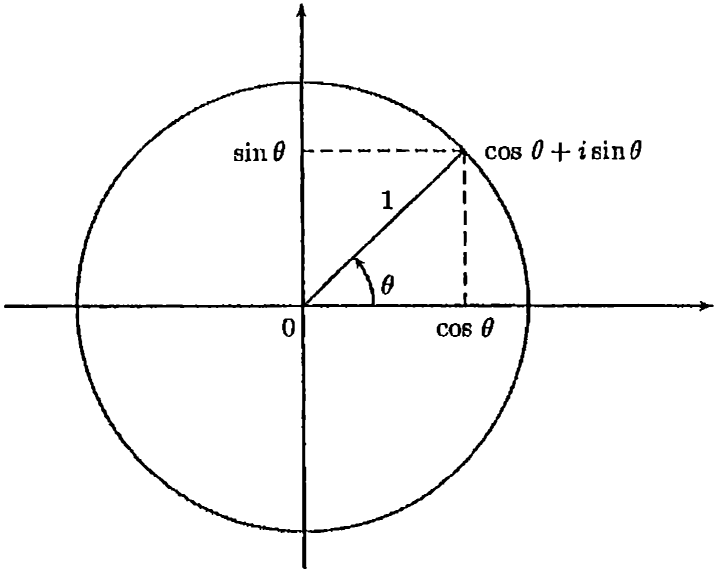
$$a = \rho\cos\theta \quad , \quad b = \rho\sin\theta.$$

Ejemplo 13.5. En la tabla siguiente pueden observarse algunos cálculos de módulos y argumentos (grafique los números y chequee los cálculos: ejercicio 13.1):

coordenadas cartesianas	módulo	argumento
1	1	0
$1+i$	$\sqrt{2}$	$\frac{\pi}{4}$
$1+i\sqrt{3}$	2	$\frac{\pi}{3}$
-1	1	π
$-i$	1	$\frac{3\pi}{2}$

13.3. Exponencial compleja

Un caso particular fundamental de representación en coordenadas polares es el de cualquier complejo $z = \cos\theta + i\sin\theta$ situado sobre el **círculo unidad**:



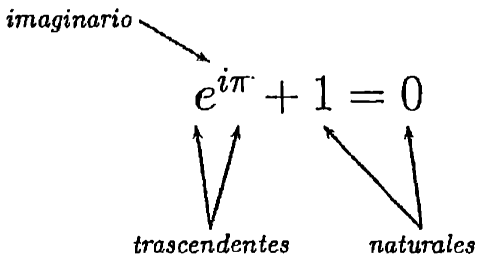
Se trata de una situación sencilla, pero que da lugar a una de las más importantes definiciones de toda la matemática.

Definición 13.6. Para $\theta \in \mathbb{R}$, la exponencial compleja $e^{i\theta}$ se define por

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

De esta manera, la exponencial $e^{i\theta}$ recorre el círculo unidad cuando θ recorre $\mathbb{R}$. En realidad, cuando θ recorre cualquier intervalo de longitud 2π, la exponencial recorre *una vez* el círculo. Al recorrer todo $\mathbb{R}$, la exponencial recorre entonces *infinitas veces* el círculo unidad. Es una función que está así *muy lejos* de ser 1-1, y su inversa (el logaritmo complejo) está *muy lejos* de existir como función. Para solventar esos problemas de «multiformidad» y poder trabajar con buenas funciones «uniformes» de variable compleja, Riemann introdujo sus famosas *superficies de Riemann*, una de las construcciones más profundas de la matemática y fuente inagotable de nuevos desarrollos a lo largo de todo el siglo XX. Se trata de un mundo fascinante, con conexiones sorprendentes que van desde la teoría de números hasta la cosmología, a descubrir en cursos posteriores (VARIABLE COMPLEJA, SUPERFICIES DE RIEMANN, GEOMETRÍA ALGEBRAICA, TEORÍA DE CATEGORÍAS).

Para el caso $\theta = \pi$, la exponencial compleja produce el resultado $e^{i\pi} = \cos\pi + i\sin\pi = -1 + i0 = -1$, es decir



La expresión recién consignada, $e^{i\pi} + 1 = 0$, se denomina la **fórmula de Euler**, y ha sido considerada por muchos como el «más bello teorema» de las matemáticas. En el camino aquí adoptado, no se trata realmente de un teorema, sino, en realidad, de un caso particular de una definición. Sin embargo, *dependiendo* de las definiciones de las cuales se parta, la fórmula de Euler puede adquirir un contenido matemático relevante y nada trivial. En

particular, si definiésemos (como lo hizo Euler[4]) la exponencial y las funciones trigonométricas mediante *series infinitas*, la fórmula de Euler resultaría mucho más misteriosa y difícil de probar (algo a lo que podrá acercarse el estudiante en un curso posterior como SUCESIONES Y SERIES).

La fórmula de Euler merece realmente el apelativo de fórmula «extraordinariamente bella» (o «más bella de la matemática» si se desea), pues expresa en una forma sorprendentemente simple *el paso de lo trascendente a lo natural, mediante el reino de lo imaginario*! En efecto, los paradigmas de la trascendencia, los números e y π (ver ejemplo 11.3.(iii)) son transformados, mediante la exponenciación imaginaria, en los paradigmas mismos de la naturalidad: los números 1 y 0. Para quien tenga la fortuna de acercarse a la matemática, la profundidad de ese tránsito produce, y seguirá produciendo, un hondo sentimiento de misterio, veneración, recogimiento y maravilla ante los abismos insondables de la naturaleza.

La fórmula de Euler ejemplifica vistosamente la forma en la que el conocimiento matemático, una vez más, *trasciende sus limitantes*. Con la fórmula de Euler, el *paso* del 0 al 1 (en las matemáticas elementales) se realiza a través de la *composición* (en las matemáticas avanzadas) de objetos trascendentes (e, π) e imaginarios (i). La matemática encarna así incesantes **tránsitos** entre lo real y lo ideal, entre lo elemental y lo complejo, y toda su riqueza radica precisamente en su excepcional capacidad para poder definir y sortear las **obstrucciones** permanentes que emergen en esos tránsitos.

Mediante la exponencial compleja, las representaciones cartesianas y polares de los complejos se enlazan cómodamente:

$$z = a + ib = \rho\cos\,\theta + i\rho\sin\theta = \rho(\cos\,\theta + i\sin\theta) = \rho e^{i\theta}.$$

Entonces, la multiplicación de dos números complejos en forma polar resulta ser inmediata: si $z = \rho e^{i\theta}$ y $z' = \rho' e^{i\theta'}$

$$zz' = \rho e^{i\theta}\rho' e^{i\theta'} = \rho\rho' e^{i\theta} e^{i\theta'} = \rho\rho' e^{i(\theta+\theta')}.$$

---

4 Leonhard Euler (Suiza, 1707-1783) fue uno de los mayores matemáticos de la historia. Sus trabajos en el análisis de las sucesiones y series infinitas expandieron de manera definitiva el conocimiento matemático. Matemático universal, sus aportes en teoría de números, geometría y combinatoria se adelantaron a menudo a su época.

De esta manera, el *módulo de un producto* de números complejos es el producto de los módulos, y el *argumento del producto* es la suma de los argumentos (módulo 2π).

Con observaciones como éstas, puede aprovecharse *el paso a través de los complejos* para demostrar resultados acerca de naturales. Por ejemplo, puede demostrarse fácilmente que un producto de dos sumas de cuadrados de naturales es a su vez una suma de cuadrados de naturales (ejercicio 13.3). La *generalización* de esta situación ha sido una de las tareas mayores de grandes campos de la matemática (como la GEOMETRÍA ALGEBRAICA o la TEORÍA ANALÍTICA DE NÚMEROS), que han culminado por ejemplo en la (muy difícil) prueba del gran Teorema de Fermat, según Wiles[5].

Mediante la exponencial compleja, pueden obtenerse inmediatamente también todas las *fórmulas trigonométricas* usuales (para las cuales no se requiere, por tanto, ningún tipo de memorización). Por ejemplo, el hecho de que el módulo de $e^{i\theta}$ es 1 (pues está en el círculo unidad) da lugar a la fórmula trigonométrica fundamental

$$\cos^2\theta + \sin^2\theta = 1.$$

Por otro lado, consideremos los siguientes dos desarrollos para $(e^{i\theta})^2$:

$$(e^{i\theta})^2 = e^{i2\theta} = \cos 2\theta + i \sin 2\theta$$

$$(e^{i\theta})^2 = (\cos\theta + i\sin\theta)^2 = (\cos^2\theta - \sin^2\theta) + i(2\sin\theta\cos\theta).$$

Al identificar las partes reales e imaginarias de las dos expresiones, se obtienen las fórmulas trigonométricas del ángulo doble

$$\cos 2\theta = \cos^2\theta - \sin^2\theta \quad , \quad \sin 2\theta = 2\sin\theta\cos\theta.$$

---

[5] Andrew Wiles (Inglaterra, n. 1953) logró demostrar en 1995 el gran Teorema de Fermat, según el cual la *única* manera de resolver la ecuación $x^n + y^n = z^n$ con naturales no nulos se logra para los exponentes $n = 1$ (trivial) y $n = 2$ (ternas de naturales que cumplan el teorema de Pitágoras). Desde el siglo XVII, cuando Fermat enunció (y creyó erróneamente demostrar) su teorema, hasta finales del siglo XX, las enormes *obstrucciones* que surgieron al tratar de demostrar el teorema dieron lugar a muchas de las herramientas más potentes inventadas en matemáticas.

13.4. Ejercicios

13.1. Dibuje las representaciones cartesianas y calcule las coordenadas polares de los números complejos presentados en el ejemplo 13.5.

13.2. Calcule las formas polares de $\frac{1}{i}$ y de $\frac{1}{1+i}$.

13.3. Si $a, b, c, d \in \mathbb{N}$, encuentre explícitamente $x, y \in \mathbb{N}$ tales que $(a^2 + b^2)(c^2 + d^2) = x^2 + y^2$. Ayuda: piense en cuadrados de módulos de números complejos.

13.4. Demuestre la fórmula de De Moivre (donde $n \in \mathbb{N}$, $\theta \in \mathbb{R}$):

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$

13.5. Utilizando dos desarrollos diferentes de $(e^{i\theta})^4$, demuestre que

$$\cos 4\theta = \cos^4\theta - 6\cos^2\theta\sin^2\theta + \sin^4\theta.$$

13.6. Utilizando las formas polares de los números complejos, encuentre todas las soluciones de las ecuaciones siguientes, y represéntelas en el plano complejo:

(i) $z^3 + 1 = 0$

(ii) $z^5 = 1$

(iii) $z^8 = \frac{1+i}{\sqrt{3}-i}$.

13.7. Sea $K = \{a + ib : a, b \in \mathbb{Z}\}$. Realice un dibujo de K sobre el plano complejo. Dados $u, v \in K$ con $v \neq 0$, demuestre que existen $q, r \in K$ tales que

$$u = qv + r \quad , \quad |r| < |v| \qquad (*)$$

(K se llama el conjunto de los enteros de Gauss; el resultado obtenido es el algoritmo de división euclidiana para K; $|z|$ es el módulo usual en los complejos). Ayuda: considere $\frac{u}{v}$ en el conjunto de los complejos, muestre que $\frac{u}{v} = x + iy$ con $x, y \in \mathbb{Q}$, muestre que existen $m, n \in \mathbb{Z}$ tales que $|x - m| \leq \frac{1}{2}$ y $|y - n| \leq \frac{1}{2}$, y defina $q = m + in$, $r = u - qv$. Muestre que los números así construidos verifican las conclusiones deseadas (pertenecer a K y verificar la condición (*): ecuación entre números y desigualdad estricta entre módulos).

Capítulo 14

Más sobre complejos

Contenido

14.1. Propiedades del conjunto de los complejos . . . 152
14.2. Ejemplos de funciones de variable compleja . . 154
14.3. El teorema fundamental del álgebra 157
14.4. Ejercicios 160

En este último capítulo, observamos cuáles propiedades de los conjuntos de números han cambiado (o se han preservado) con la introducción de los números complejos, ampliamos algunas informaciones sobre el comportamiento *sintético* de los complejos (conocimiento de sus funciones), y demostramos la propiedad fundamental de $\mathbb{C}$: el hecho de que *todo* polinomio no constante en $\mathbb{C}[X]$ posee *siempre* raíces en $\mathbb{C}$. Este último resultado, conocido como el «teorema fundamental del álgebra», sirve de adecuado colofón para el curso de FUNDAMENTOS, pues, por un lado, maneja una cierta *sofisticación demostrativa* a la que debe haber podido acceder el estudiante, pero sobre todo, por otro lado, *abre* compuertas para el desarrollo futuro del estudiante, en una Carrera que no dejará de sorprenderlo y de exigirle.

14.1. Propiedades del conjunto de los complejos

Las propiedades esenciales del conjunto de los números complejos habían sido ya anunciadas en la tabla de la sección 10.1. Las propiedades de la *suma* en $\mathbb{C}$ (asociatividad, conmutatividad, existencia de neutro (0), existencia de

inversos) se deducen *directamente* de las buenas propiedades de la suma en $\mathbb{R}$. Para la suma, es útil manejar la representación de los complejos en coordenadas *cartesianas*. Por ejemplo, la conmutatividad de la suma en $\mathbb{C}$ se deriva de las ecuaciones $(a+ib)+(c+id) = (a+c)+i(b+d) = (c+a)+i(d+b) = (c+id)+(a+ib)$: las igualdades primera y última se deben a la definición de la suma en $\mathbb{C}$, y la segunda igualdad se debe a (un uso doble de) la conmutatividad de la suma en $\mathbb{R}$. Dejamos que el estudiante verifique las demás propiedades para la suma en $\mathbb{C}$ (ejercicio 14.1).

Las propiedades de la *multiplicación* en $\mathbb{C}$ (asociatividad, conmutatividad, existencia de neutro (1), existencia de inversos para complejos no nulos, distributividad de la multiplicación con respecto a la suma) se derivan también de las buenas propiedades de $\mathbb{R}$, pero estas pruebas no sólo usan las propiedades respectivas de la multiplicación en $\mathbb{R}$, sino *también* aquellas de la suma. Estas pruebas son ejemplos sencillos de pruebas *mixtas*: los *mixtos* en matemáticas aparecen por doquier, y constituyen la profunda razón de ser de muchas construcciones que acercan *polaridades* opuestas (discreto y continuo, finito e infinito, algebraico y trascendente, etc.). Para la multiplicación, pueden realizarse también pruebas con complejos en forma cartesiana, pero resulta ser mucho más cómodo en cambio trabajar con sus representaciones *polares*. Por ejemplo, la conmutatividad de la multiplicación en $\mathbb{C}$ se deriva de las ecuaciones $\rho e^{i\theta}\rho' e^{i\theta'} = \rho\rho' e^{i\theta}e^{i\theta'} = \rho\rho' e^{i(\theta+\theta')} = \rho' \rho e^{i(\theta'+\theta)} = \rho' \rho e^{i\theta'}e^{i\theta} = \rho' e^{i\theta'}\rho e^{i\theta}$: las igualdades primera y última se deben a la definición de multiplicación en forma polar, la segunda y la penúltima se deben a la propiedad fundamental de la exponencial (transformar sumas en productos), y la igualdad central *combina* simultáneamente la conmutatividad de la multiplicación en $\mathbb{R}$ (para los módulos) y la conmutatividad de la suma en $\mathbb{R}$ (para los argumentos). El estudiante verificará, en forma similar, las demás propiedades para la multiplicación en $\mathbb{C}$ (ejercicio 14.2).

Hemos señalado, a lo largo de este texto, el *carácter pendular* de la matemática: *dependiendo de las problemáticas en juego*, ciertos conceptos y objetos son más apropiados que otros, y, a menudo, lo que por un lado se gana, por otro lado se pierde. Con los complejos, como veremos en la sección 14.3, ganamos *todo lo posible* en la resolución de ecuaciones polinomiales. Pero, por otro lado, perdemos una característica fundamental de *todos* los conjuntos anteriores $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R})$: sus *órdenes* bien comportados. De hecho, en $\mathbb{C}$ *no existe* un orden que extienda al orden de $\mathbb{R}$ y que se comporte bien con respecto a las operaciones (es decir, que sea una relación de orden *congruente* con las operaciones: véanse los comentarios sobre «congruencias» después de la definición 8.4). Éste es un resultado delicado, que se encuentra

relacionado con la imposibilidad de definir una noción adecuada de *positividad* para los números complejos, y que puede ser demostrado en algún curso posterior de TEORÍA DE MODELOS (sin embargo, para indicaciones, véase el ejercicio 14.5). Una vez más, nos acercamos aquí a ciertos linderos del *no*, sobre los que la matemática tiene mucho que decir. Por otro lado, en un nuevo movimiento pendular, la *inexistencia misma* de un orden congruente en $\mathbb{C}$ ha adquirido (en la TEORÍA DE MODELOS contemporánea) una importancia inesperada. El *vuelco* de la situación provee una profunda «estabilidad» a $\mathbb{C}$, de la que *no* gozan los subconjuntos ordenados usuales de $\mathbb{R}$.

Con respecto a las demás propiedades de $\mathbb{C}$ señaladas en la tabla 10.1, la «completitud analítica» de $\mathbb{C}$ (*todos los límites*) se deriva fácilmente de la completitud de $\mathbb{R}$ (el estudiante revisará y profundizará estas ideas en cursos posteriores de ANÁLISIS y TOPOLOGÍA). En cuanto a la «completitud algebraica» de $\mathbb{C}$ (*todas las raíces*), remitimos a la sección 14.3.

14.2. Ejemplos de funciones de variable compleja

Las funciones de variable compleja son funciones $f : \mathbb{C} \longrightarrow \mathbb{C}$. Algunas de esas funciones (las funciones «analíticas», a estudiarse con cuidado en el curso de VARIABLE COMPLEJA) poseen propiedades de *coherencia* extremadamente fuertes: *lisura* en *un* nivel (primera «derivada») generando lisura en *todos* los niveles (todas las «derivadas»), conocimiento en una *región* generando *determinación* de la función en un *punto* («fórmula integral de Cauchy»), pequeñas variaciones en los argumentos generando *pegamientos* de las variaciones de las funciones («continuación analítica»), etc. El magnífico comportamiento de esas funciones de variable compleja contrasta con el comportamiento *totalmente errático* que pueden tener en cambio las funciones de variable real (curso de ANÁLISIS). En lo que sigue, observaremos algunos ejemplos de funciones de variable compleja.

Las funciones módulo y argumento, que encapsulan la información de los complejos en coordenadas polares, son de gran utilidad:

$$|\ |: \mathbb{C} \longrightarrow \mathbb{R}^+ : z \mapsto |z|$$

$$arg : \mathbb{C} \longrightarrow [0, 2\pi[: z \mapsto arg(z).$$

Como $\mathbb{R}^+$ y $[0, 2\pi[$ son subconjuntos de $\mathbb{C}$, estas funciones pueden considerarse como funciones de $\mathbb{C}$ en $\mathbb{C}$, y, aunque no son funciones que se comportan «bien» en el sentido recién mencionado, su comportamiento estructural alge-

braico es muy útil. En particular, las siguientes propiedades (ejercicio 14.3) serán utilizadas ampliamente en la próxima sección:

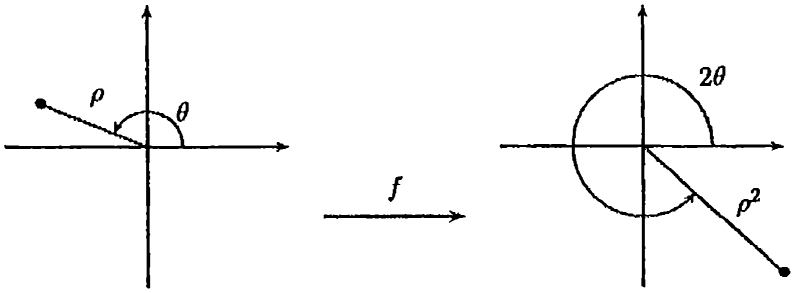
$$|z+z'| \leq |z|+|z'| \quad , \quad |zz'| = |z||z'|$$

$$arg(zz') = arg(z) + arg(z') \quad , \quad arg(z^n) = n\, arg(z) \quad \text{(módulo } 2\pi)$$

(donde la suma o la multiplicación «módulo 2π» consiste en sumar o multiplicar de la forma usual, y luego tomar el resto en la división por 2π). Las funciones módulo y argumento están *muy lejos* de ser 1-1 (¿por qué?), pero, *combinadas* al tiempo, sí caracterizan de manera única a un complejo.

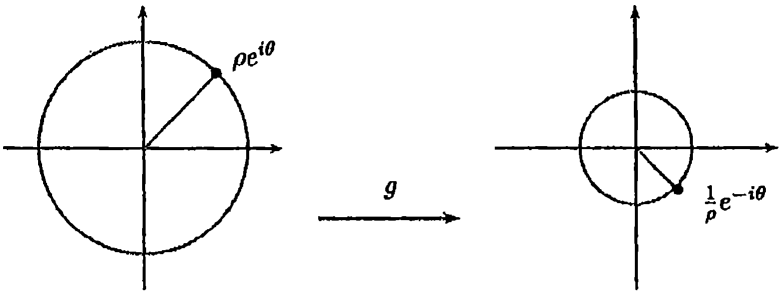
Al considerar otras funciones de variable compleja se obtiene un salto *genuino*, con *nuevas* gráficas. Esas gráficas no pueden dibujarse en un plano cartesiano simple, pues involucran al menos cuatro dimensiones reales ($\mathbb{C} \times \mathbb{C} \sim \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$), pero pueden proveerse *fragmentos* de esas gráficas. Presentamos a continuación algunos fragmentos de gráficas de funciones sencillas.

Ejemplo 14.1. (i) *Función cuadrática*: $f : \mathbb{C} \longrightarrow \mathbb{C} : z \mapsto z^2$.



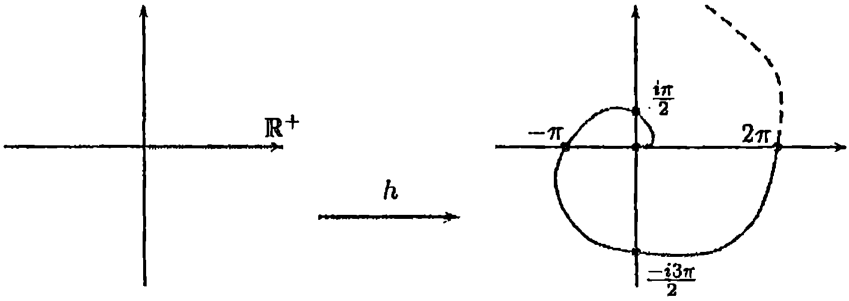
La función cuadrática eleva módulos al cuadrado y dobla argumentos. Puede chequearse (ejercicio 14.4) que la función cuadrática compleja es una *biyección* del plano estrictamente superior $P^{>} = \{z \in \mathbb{C} : Im(z) > 0\}$ *sobre* todo el plano complejo $\mathbb{C}$ excepto el eje real positivo $\mathbb{R}^+$. En forma similar, la función cuadrática compleja produce otra biyección del plano superior $P^{\geq} = \{z \in \mathbb{C} : Im(z) \geq 0\}$ excepto el eje real positivo *sobre* $\mathbb{C} - \{0\}$.

(ii) *Función inversa*: $g : \mathbb{C} - \{0\} \longrightarrow \mathbb{C} : z \mapsto 1/z$.



La función inversa invierte módulos multiplicativamente, e invierte argumentos aditivamente. Puede chequearse (ejercicio 14.4) que la función inversa envía círculos en círculos (en particular, envía el círculo de radio ρ en el círculo de radio $1/\rho$).

(ii) *Función espiral*: $h : \mathbb{C} \longrightarrow \mathbb{C} : z \mapsto ze^{iz}$.



Puede chequearse (ejercicio 14.4) que la función h envía el eje real positivo R^+ en la espiral infinita cuyo comienzo se esquematiza en la gráfica.

14.3. El teorema fundamental del álgebra

Presentamos ahora una demostración «elemental» de que todo polinomio no constante en $\mathbb{C}[X]$ posee raíces en $\mathbb{C}$. Este hecho fundamental explica la razón de ser profunda de los números complejos. Gauss[1] lo demostró por vez primera a fines del siglo XVIII, pero desde entonces ha recibido una enorme cantidad de pruebas alternativas. La demostración que realizaremos (que aparece en un ejercicio del famoso *Curso de álgebra* de Godement[2]) tiene la ventaja de usar *sólo dos* herramientas avanzadas, que pueden ser claramente explicitadas en el curso de la prueba, mientras que todos los demás argumentos incorporados en la prueba son «elementales» (uso de herramientas teóricas de bajo nivel de complejidad). Lo «elemental» no debe aquí confundirse con lo «fácil»: a menudo lo elemental puede ser bastante más difícil que lo avanzado, justamente porque en el ámbito de lo elemental no se poseen aún herramientas poderosas de pruebal

Teorema 14.2. *(Teorema fundamental del álgebra). Para todo polinomio no constante* $P(X) \in \mathbb{C}[X]$ *existe* $a \in \mathbb{C}$ *tal que* $P(a) = 0$.

---

1 Carl Friedrich Gauss (Alemania, 1777-1855) ha sido denominado el «príncipe de las matemáticas» debido a sus profundas contribuciones en todos los campos de la matemática. Gauss fue el primero en demostrar completamente el teorema fundamental del álgebra (en su tesis doctoral de 1799), del que produjo después al menos otras cuatro pruebas diferentes. Sus *Disquisiciones aritméticas* constituyen el modelo por excelencia de la matemática «clásica» (cercana estéticamente a lo que representa un Beethoven en la música). Gauss fue un pionero en muchos dominios (particularmente, en las geometrías no euclídeas), pero su talante algo conservador impidió que se atreviera a publicar ideas demasiado «revolucionarias».

2 Roger Godement (Francia, n. 1921) es uno de los brillantes matemáticos franceses de mediados del siglo XX. Su texto *Topología algebraica y teoría de haces* (1958) estableció sobre bases firmes la teoría de haces, frontera entre la matemática moderna y la matemática contemporánea. Su célebre *Curso de álgebra* ha sido fuente permanente de *educación* y *elegancia* para generaciones enteras de matemáticos.

Demostración. Sea $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{C}[X]$, con $a_n \neq 0$, $n \geq 1$. Como los coeficientes de P son números complejos, podemos considerar la función f de variable compleja definida por $f : \mathbb{C} \longrightarrow \mathbb{C} : z \mapsto f(z) = a_0 + a_1z + a_2z^2 + \cdots + a_nz^n$. Utilizando **propiedades de funciones continuas** (he aquí el *primer paso avanzado* que solicitamos al estudiante aceptar por el momento: completará su formación en un curso de ANÁLISIS o de TOPOLOGÍA), se puede mostrar que el ínfimo de $|f|$ se obtiene en un punto específico a, es decir, que existe $a \in \mathbb{C}$ tal que $inf_{z\in\mathbb{C}}|f(z)| = |f(a)|$. Vamos a demostrar que $f(a) = 0$, por tanto a será una raíz de $P(X)$.

La prueba procede *por contradicción* (el estudiante habrá ya observado que muchas de las pruebas centrales del curso de FUNDAMENTOS utilizan este recurso: teoremas de Cantor, identidad de Bézout, etc.). Supongamos que $f(a) \neq 0$. Podemos entonces considerar la función de variable compleja $g : \mathbb{C} \longrightarrow \mathbb{C}$ definida por $g(z) = \frac{f(z+a)}{f(a)}$. Se tiene $g(0) = 1$ (inmediato) y

$$\text{para todo } z \quad |g(z)| \geq 1 \quad (*),$$

pues $|f(z + a)| \geq |f(a)|$, ya que $|f(a)|$ es el mínimo valor posible para $|f|$. Procederemos en la prueba, y llegaremos a una contradicción con (*).

Al tener $g(0) = 1$, la función g puede desarrollarse polinomialmente en la forma $g(z) = 1 + b_qz^q + \cdots + b_nz^n$ con algún $b_q \neq 0$ (he aquí el *segundo paso avanzado* que incluimos: **desarrollos en serie de Taylor**, a completar en un curso de ANÁLISIS o de VARIABLE COMPLEJA). De ahora en adelante, sólo manejaremos razonamientos «elementales», aprovechando en particular las propiedades de las funciones módulo y argumento.

Tenemos $|g(z) - 1 - b_qz^q| = |b_{q+1}z^{q+1} + \cdots + b_nz^n| \leq |b_{q+1}z^{q+1}| + \cdots + |b_nz^n| = |z^{q+1}|(|b_{q+1}| + \cdots + |b_n||z^{n-(q+1)}|)$ (la primera desigualdad utiliza la propiedad $|z + z'| \leq |z| + |z'|$, la última igualdad utiliza distributividad y la propiedad $|zz'| = |z||z'|$). Si $|z| \leq 1$, se tiene que $|b_{q+1}| + \cdots + |b_n||z^{n-(q+1)}| \leq |b_{q+1}| + \cdots + |b_n|$. Definamos M por $M = |b_{q+1}| + \cdots + |b_n|$ (como $b_n \neq 0$, $M > 0$). De los cálculos realizados en este párrafo se tiene que $|g(z) - 1 - b_qz^q| \leq M|z|^{q+1}$ en el caso en que

$$|z| \leq 1 \quad \text{(condición A)}.$$

Observemos ahora $|g(z)|$. Utilizando la desigualdad de módulos $|z| \leq |z - z'| + |z'|$, se tiene que $|g(z)| \leq |g(z) - 1 - b_qz^q| + |1 + b_qz^q|$, y, por la desigualdad obtenida en el párrafo anterior, $|g(z)| \leq |g(z) - 1 - b_qz^q| + |1 + b_qz^q| \leq M|z|^{q+1} + |1 + b_qz^q|$.

Si lográramos escoger z tal que

$$b_q z^q = r \in \mathbb{R}, \quad -1 \leq r \leq 0 \quad \text{(condición B)},$$

tendríamos que $|1 + b_q z^q| = |1 + r| = 1 - |r|$ (chequee esta última igualdad: requiere usar r real en el intervalo [-1,0]).

Si, además, lográramos escoger z tal que

$$M|z| < |b_q| \quad \text{(condición C)},$$

tendríamos que $M|z|^{q+1} < |b_q z^q|$ (la desigualdad estricta es crucial).

Combinando las anteriores ecuaciones y desigualdades, tendríamos, para el caso de un número complejo z que verificara *simultáneamente* las condiciones (A), (B) y (C),

$$|g(z)| \leq M|z|^{q+1} + |1 + b_q z^q| < |b_q z^q| + 1 - |b_q z^q| = 1$$

es decir,

$$|g(z)| < 1$$

contradiciendo la propiedad inicial (*). Si podemos encontrar *algún* complejo z que verifique las tres condiciones (A), (B), (C), tendremos entonces la contradicción deseada.

Ahora bien, la búsqueda de un tal z sólo depende de propiedades elementales de módulos y argumentos. En efecto, para verificar la condición (B), hay que verificar primero que $b_q z^q$ sea igual a un real r negativo, es decir que su argumento sea igual a π. Pero $arg(b_q z^q) = \pi$ equivale a decir $arg(b_q) + q\ arg(z) = \pi$ (por las propiedades del argumento señaladas en el ejercicio 14.3), lo que equivale a decir

$$arg(z) = \frac{\pi - arg(b_q)}{q} \qquad \text{(condición B1)}.$$

Para terminar de verificar la condición (B), hay que verificar que $-1 \leq r \leq 0$, lo que equivale a $|r| = |b_q||z|^q \leq 1$, lo que equivale a decir

$$|z| \leq \sqrt[q]{\frac{1}{|b_q|}} \qquad \text{(condición B2)}.$$

Por otro lado, para verificar la condición (C), basta con tener la condición inmediatamente equivalente

$$|z| < \frac{|b_q|}{M} \qquad \text{(condición C1)}.$$

Cualquier número complejo que verifique las condiciones (A), (B1), (B2) y (C1) verificará entonces las condiciones (A), (B) y (C), y nos producirá la contradicción deseada. Ahora bien, la verificación simultánea de las condiciones (A), (B2) y (C1) se consigue simplemente al pertenecer (estrictamente) al *más pequeño* de los tres *discos* concéntricos alrededor del origen, de radios respectivos 1, $\sqrt[q]{\frac{1}{|b_q|}}$ y $\frac{|b_q|}{M}$. Y verificar la condición (B1) consiste simplemente en situarse sobre el *radio* cuyo argumento es igual a $\frac{\pi - arg(b_q)}{q}$.

Así, no sólo existe *un* complejo z que verifique las condiciones (A), (B1), (B2), (C1) (y también, por tanto, las condiciones (A), (B) y (C)), sino que existen *infinitos* complejos con esa propiedad. La contradicción se asegura así de una manera muy fuerte.

□

14.4. Ejercicios

14.1. Utilizando las representaciones cartesianas de los complejos, demuestre las buenas propiedades de la suma en $\mathbb{C}$: asociatividad, conmutatividad, existencia de neutro (0), existencia de inversos. Explique cuidadosamente la razón de ser de *cada* igualdad que usted escriba. Intente hacer esas pruebas con las representaciones polares y reflexione sobre las *obstrucciones* que encuentre.

14.2. Utilizando las representaciones polares de los complejos, demuestre las buenas propiedades de la multiplicación en $\mathbb{C}$: asociatividad, conmutatividad, existencia de neutro (1), existencia de inversos para complejos no nulos, distributividad de la multiplicación con respecto a la suma. Explique cuidadosamente la razón de ser de *cada* igualdad que usted escriba. Intente hacer esas pruebas con las representaciones cartesianas y reflexione sobre las *obstrucciones* que encuentre.

14.3. Demuestre las propiedades de módulo y argumento señaladas en el texto:

$$|z+z'| \leq |z|+|z'| \quad , \quad |zz'| = |z||z'|$$

$$arg(zz') = arg(z) + arg(z'), \quad arg(z^n) = n\, arg(z) \quad \text{(módulo } 2\pi).$$

14.4. Verifique las diversas aserciones acerca de las transformaciones de regiones del plano complejo señaladas en el ejemplo 14.1: imágenes bajo las funciones cuadrática, inversa y espiral.

14.5. Muestre que no existe un orden estricto $<$ en $\mathbb{C}$ que verifique las siguientes propiedades: (1) si $x \neq 0$ entonces $x > 0$ o $x < 0$; (2) $x < 0$ si y sólo si $-x > 0$; (3) $x > 0$ implica $x^2 > 0$. Ayuda: proceda por contradicción, y muestre que si un tal orden existe, necesariamente $1 > 0$; luego, considerando $x = i$, demuestre que necesariamente $-1 > 0$, y obtenga una contradicción.

Bibliografía anotada

Es útil leer a grandes matemáticos que hayan sabido escribir textos didácticos. Para el caso del curso de FUNDAMENTOS, pueden consultarse los siguientes tres trabajos (ordenados por nivel de dificultad creciente):

1. Richard Courant, Herbert Robbins, *Qué es la matemática*, Madrid: Aguilar, 1967.

Los capítulos 1 y 2 cubren algo de conjuntos, infinitud y sistemas de números. Los demás capítulos van más allá de lo que se ofrece aquí en un curso de FUNDAMENTOS. Este texto es un *clásico* de la divulgación matemática, que nos ha legado uno de los exponentes mayores (Courant) de la escuela de Hilbert.

2. W.S. Anglin, J. Lambek, *The Heritage of Thales*, New York: Springer, 1995.

La primera parte presenta un muy original recorrido por la historia de las matemáticas, con numerosos problemas tratados en el curso de FUNDAMENTOS. La segunda parte presenta los conjuntos de números, de nuevo con perspectivas originales, y abre muchas otras compuertas. Lambek es uno de los grandes inventores en la teoría de categorías, y un matemático de primera línea.

3. Solomon Feferman, *The Number Systems*, Reading: Addison-Wesley, 1964.

Este texto cubre *exactamente* el mismo temario del curso de FUNDAMENTOS, pero la presentación es mucho más rigurosa y completa. Puede ser algo difícil en una primera aproximación, pero sirve de excelente complemento para el *buen* estudiante del curso de FUNDAMENTOS. Feferman es uno de los lógicos mayores de la segunda mitad del siglo XX, y editor de la obra completa de Gödel.

Más allá de los textos *clásicos* anteriores, muy recomendados, han aparecido múltiples trabajos de nivel intermedio que cubren las temáticas del curso de FUNDAMENTOS. En especial, el siguiente texto se ha venido usando con éxito en el Departamento de Matemáticas de la Universidad Nacional - Sede Bogotá:

4. Ethan Bloch, *Proofs and Fundamentals: A First Course in Abstract Mathematics*, Boston: Birkhauser, 2000.

Otros textos de nivel (y valor conceptual) intermedio pueden ser:

5. Carl Allendoerfer, *Fundamentals of Freshman Mathematics*, New York: McGraw Hill, 1959.

6. Moses Richardson, *Fundamentals of Mathematics*, New York: MacMillan, 1966.

7. Elbridge Vance, *Fundamentals of Mathematics*, London: Addison-Wesley, 1960.

Como complemento al curso de FUNDAMENTOS, las lecturas históricas son primordiales. Los tres textos siguientes proveen visiones de conjunto. El trabajo de Bell, en particular, otorga una motivación potente para querer desarrollar estudios de matemáticas.

8. Eric Temple Bell, *Los grandes matemáticos*, Losada: Buenos Aires, 1948.

9. Florian Cajori, *A History of Mathematics*, New York: MacMillan, 1955.

10. Carl Boyer, *A History of Mathematics*, New York: Wiley, 1968.

Finalmente, el estudiante debe ir mezclando los grandes ejemplos (Courant, Lambek, Feferman), con mediaciones más elementales (los textos de Bloch o Allendoerfer, así como este texto), y con manuales puramente mecánicos y formulísticos. Éste es el caso de la serie Schaum, nada recomendable como *única* fuente bibliográfica, pero útil en cambio como insumo *menor*. En particular, puede servir de ayuda el texto:

11. Seymour Lipschutz, *Teoría de conjuntos y temas afines*, México: McGraw-Hill, 1970.

Fundamentos de matemáticas
se terminó de reimprimir y encuadernar
en marzo de 2012, con un
tiraje de 300 ejemplares,
sobre papel bond blanco de 75 g.
Bogotá, D. C., Colombia.